



Proposta Comercial

DEFENSORIA PÚBLICA DO ESTADO DE MINAS GERAIS

PREGÃO ELETRÔNICO Nº 1441003 27/2026

Processo: 1441003 000027/2026

**DATA DA SESSÃO PÚBLICA: 27/04/2026, às 10:00h - Horário de
BRASÍLIA-DF.**

Nº Proposta: 27/04/2026

Versão Proposta: 01 Brasília, 27 de abril de 2026

1. Apresentação da Empresa

1.1. Sobre nós

A Alltech Soluções em Tecnologia é uma empresa focada em soluções e serviços de TI, com mais de 08 anos de experiência no mercado nacional no setor público, com sede em Brasília/DF e atuação em 13 Estados brasileiros. Especializada em consultoria em TI, desenvolvimento de aplicações, automação, segurança da informação, cloud, gestão de TI, DevOps e suporte técnico, a Alltech conta com uma equipe de profissionais altamente capacitados e tecnologias de ponta para garantir a eficiência e a segurança dos serviços prestados. Temos como objetivo principal ajudar nossos clientes a alcançarem seus objetivos de negócio por meio da tecnologia, oferecendo soluções inovadoras e personalizadas para cada necessidade.

1.2. Certificação de Transparência CertiGov



A Alltech Soluções em Tecnologia, acaba de conquistar a certificação de transparência **CertiGov**, na classe bronze. O selo atesta as ações de integridade da empresa em seus processos, política e cultura ética. Com o certificado, a Alltech fomenta a segurança de sua cadeia de atuação para vendas ao governo, e se antecipa à demanda crescente por práticas de compliance aos fornecedores dos setores público e privado.

As empresas que conquistam o **CertiGov** demonstram seu posicionamento contra a corrupção e contra o suborno, demonstrando que tem os conceitos disseminados em sua organização e colaboradores, e implantam boas práticas para reduzir os riscos de envolvimento em ações ilícitas. O processo de certificação da Alltech Soluções em Tecnologia incluiu uma avaliação detalhada dos processos, riscos e aderência a rigorosos padrões de integridade e treinamentos.

2. Nossos Parceiros



3.1 Valor da Proposta:

DO OBJETO: O objeto do presente contrato é aquisição de ativos de rede e Solução de NAC, sob a forma de entrega parcelada, conforme condições do Termo de Referência.

O prazo de vigência da contratação é de 12 (doze) meses contados da publicação do contrato no Portal Nacional de Contratações Públicas - PNCP, na forma do art. 105 da Lei nº 14.133, de 2021.

PROPOSTA COMERCIAL - LOTE 02							
LOTE	ITEM	Código do item no SIAD	DESCRIÇÃO/PRODUTO	UNIDADE	QTD	VALOR UNITÁRIO	VALOR TOTAL
2	1	101540	LICENCA PERPETUA DE FERRAMENTA DE CONTROLE DE ACESSO A REDE NETWORK ACCESS CONTROL (NAC)	Unidade	1	R\$ 595.138,64	R\$ 595.138,64
	2	152510	LICENCA ADICIONAL DE SOLUCAO DE CONTROLE DE ACESSO A REDE (NAC): AUTENTICACAO, PROFILING E ACESSOS SIMULTANEOS	Unidade	6	R\$ 107.819,03	R\$ 646.914,17
VALOR TOTAL GLOBAL							R\$ 1.242.052,81

Valor por extenso: R\$1.242.052,81 (Um milhão duzentos e quarenta e dois mil e cinquenta e dois reais e oitenta e um centavos).

Detalhamento Técnica:

LOTE 2 - Item 1 – Licenciamento para 1000 dispositivos simultâneos.

- FNC-CAX-VM - LICENÇA DE SOFTWARE - CONTROLE E APLICATIVO FORTINAC SERVIDOR VM DE PROXIMA GERAÇÃO VMWAREHYPERVAWSAZUREKVM.
- Garantia de 60 meses conforme termo de referência.

LOTE 2 - Item 2 – Add-on de 500 dispositivos simultâneos

- LIC-FNAC-PRO-100 LICENÇA DE SOFTWARE - FORTINAC PRO LICENSE FOR 100 CONCURRENT ENDPOINT DEVICES. PRO LICENSE LEVEL PROVIDES THE ULTIMATE IN VISIBILITY, CONTROL AND RESPONSE.
- Garantia de 60 meses conforme termo de referência.

Serviço de Instalação e suporte conforme termo de referência.

3.2. Condições de Pagamento:

O prazo para pagamento ao contratado e demais condições a ele referentes encontram-se definidos no EDITAL em **ANEXO I TERMO DE REFERÊNCIA – 5.3. DO PAGAMENTO** deste Edital.

Forma de pagamento:

5.3. Do Pagamento:

5.3.1 O pagamento será efetuado através do Sistema Integrado de Administração

Financeira - SIAFI/MG, por meio de ordem bancária

emitida por processamento eletrônico, a crédito do beneficiário em um dos bancos que o Contratado indicar, no prazo de até 30 (trinta) dias corridos, contados a partir da data final da liquidação a que se referir, com base nos documentos fiscais

devidamente conferidos e aprovados pelo Contratante.

5.3.1.1. A Administração deve observar a ordem cronológica nos pagamentos, conforme disposto no art. 141 da Lei Federal nº 14.133, de 2021.

5.3.2. No caso de atraso pelo Contratante, por culpa exclusiva da Administração, os valores devidos ao Contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, de acordo com a variação do IPCA.

5.3.3. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

5.3.4. Independentemente do percentual de tributo inserido pelo Contratado na planilha de custo, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

5.3.5. A CONTRATADA deve garantir a manutenção dos requisitos de habilitação previstos no Edital.

5.3.5.1. Eventuais situações de irregularidades fiscal ou trabalhista da CONTRATADA não impedem o pagamento, se o objeto tiver sido executado e atestado. Tal hipótese ensejará, entretanto, a adoção das providências tendentes ao sancionamento do contratado e rescisão contratual.

5.3.6. O Contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei

Complementar.

3.3. Validade da Proposta: Os termos e condições desta proposta são válidos por um período de 90 (noventa) dias a contar da data de sua apresentação.

3.4. Observações e Declarações: Os preços incluem taxas, impostos, seguros pertinentes, custos diretos e indiretos, tributos, encargos sociais, tributários, trabalhistas e previdenciários, seguros, taxas, lucro e outros necessários ao cumprimento integral do objeto.

Estamos cientes e concordamos com as condições contidas neste Edital e seus anexos, bem como, sob pena de desclassificação, de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo;

4. Informações Complementares

4.1. Proponente

Razão Social: Alltech Soluções em Tecnologia Ltda.

CNPJ: 21.547.011/0001-66

Endereço: SCN Quadra 01 Bloco F – Salas 802 a 810 – Ed. America Office

Tower – Brasília, DF

E-mail: mrossetto@alltechsolucoes.com.br

Telefone: (61) 3344-0236 (61) 99818-3179.

Inscrição Estadual: 07.704.559/001-89

Optante pelo Simples: Não.

Dados do Representante Legal da Empresa para assinatura do Contrato:

Nome: Murilo Rossetto

CPF/MF: 036.031.821-54

E-mail: mrossetto@alltechsolucoes.com.br

Cargo/Função: Diretor

4.2. Operação de Crédito:

Banco do Brasil S.A.

Agência: 3382-0 C/C: 6734-2

Brasília, DF, 27 de abril de 2026



Murilo Rossetto
Representante Legal
**Alltech Soluções em
Tecnologia Ltda**

ITEM	DESCRIÇÃO	REFERÊNCIA	# DA PÁGINA OU LINK	COMPROVAÇÃO / LINK
1.5.11	SOLUÇÃO DE CONTROLE DE ACESSO A REDE (NETWORK ACCESS CONTROL – NAC) – ITEM 1 / LOTE 02			
1.5.11.1	A plataforma deverá ser fornecida em formato virtual (projetado e customizado para a função de NAC) com redundância.	DE ACORDO COM A PROPOSTA COMERCIAL DE ACORDO COM A PROPOSTA TÉCNICA		
1.5.11.2	A CONTRATADA deverá informar as configurações, de hardware e softwares, necessárias para o funcionamento da solução sem que haja prejuízo na sua plena utilização e escalabilidade. Deve ser compatível com o ambiente de virtualização: VMWare versão 8.0 ou superior.	DE ACORDO COM A PROPOSTA TÉCNICA	PG 13	https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortinac.pdf
1.5.11.3	Em caso de utilização de banco de dados externo como SQL Server, Oracle ou outros, as licenças do banco de dados deverão ser fornecidas e serem perpétuas.	Não se Aplica		
1.5.11.4	Devem ser fornecidas licenças perpétuas para todas as funcionalidades da plataforma NAC. Caso alguma funcionalidade dependa de atualização periódica por subscrição, seu funcionamento não poderá ser interrompido após o vencimento da subscrição. Significa que: ao expirar o contrato, apenas as atualizações deixam de ser disponibilizadas, mas todas as funcionalidades já habilitadas devem continuar operando normalmente.	DE ACORDO COM A PROPOSTA COMERCIAL DE ACORDO COM A PROPOSTA TÉCNICA		https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/500853/high-availability
1.5.11.5	Deve ser fornecido com recursos (software e licenças) suficientes para implementar a redundância da plataforma de NAC. Além disso, deverá ser possível implementar a redundância no mesmo segmento de rede.	FortiNAC-F 7.6.0 Administration Guide High availability DE ACORDO COM A PROPOSTA COMERCIAL	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/500853/high-availability
1.5.11.6	Deve permitir a realização do backup de toda a configuração de forma manual e automática através de agendamento.	FortiNAC-F 7.6.0 Backup and Restore (FortiNAC-OS) Manual Backups Scheduling Backups	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/backup-and-restore-fortinac-os/276538/overview
1.5.11.7	Realizar o backup do banco de dados de forma manual e automática através de agendamento, em caso de uso de banco de dados interno.	FortiNAC-F 7.6.0 Backup and Restore (FortiNAC-OS) Manual Backups Scheduling Backups	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/backup-and-restore-fortinac-os/276538/overview
1.5.11.8	Deve atender aos requisitos gerais da solução, descritos neste Termo de Referência e seus Anexos.	DOCUMENTO DE COMPROVAÇÃO TECNICA		

1.5.11.9	Todas as configurações de segurança como, por exemplo, políticas/fluxos de controle de admissão à rede/NAC e estabelecimento de perfil/profiling, deverão ser realizadas em um mesmo local e devem ser válidas, no que couber, tanto para a rede WLAN quanto para a rede LAN. Não serão admitidos componentes com funções iguais para operação/configuração da LAN e WLAN em separado.	DE ACORDO COM A PROPOSTA COMERCIAL DE ACORDO COM A PROPOSTA TÉCNICA		
1.5.11.10	A solução de segurança, responsável pelos serviços de autenticação de usuários corporativos e visitantes, monitoramento das autenticações, armazenamento de logs, relatórios, e controle de acesso (NAC e profiling), será instalada nos datacenters da DPMG devendo possuir alta disponibilidade/redundância automática para todos os componentes.	DE ACORDO COM A PROPOSTA COMERCIAL DE ACORDO COM A PROPOSTA TÉCNICA		https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/500853/high-availability
1.5.11.11	Caso a solução de segurança seja composta por mais de um componente, estes devem atender tanto a rede LAN quanto WLAN de forma centralizada a fim de atender aos requisitos citados nas configurações de segurança anteriormente descritas. Entretanto, cada componente pode apresentar sua própria interface gráfica de administração.	DE ACORDO COM A PROPOSTA COMERCIAL DE ACORDO COM A PROPOSTA TÉCNICA		
1.5.11.12	Deve gerar e manter certificados digitais X.509 assinados por uma CA interna à solução e permitir a integração desta CA em uma estrutura de PKI da DPMG.	FortiNAC-F 7.6.0 Administration Guide Certificates SSL certificates Server certificates TEAP configuration Obtain a certificate from CA	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/160665/certificates https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/299581/ssl-certificates https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/691790/server-certificates https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/119792/teap-configuration https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/470693/obtain-a-certificate-from-ca
1.5.11.13	Deve implementar autenticação 802.1X para os usuários da rede com e sem fio, utilizando os seguintes métodos: EAP-TLS, PEAP-MSCHAPv2 e EAP-TTLS.	FortiNAC-F 7.6.0 Administration Guide RADIUS Virtual Servers 802.1X	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/214558/radius https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/450544/virtual-servers https://docs.fortinet.com/document/fortinac-f/7.6.0/fortiap-integration/445346/802-1x
1.5.11.14	Deve permitir a integração com RADIUS Server com suporte aos métodos EAP citados no item anterior.	FortiNAC-F 7.6.0 Administration Guide RADIUS Virtual Servers 802.1X	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/214558/radius https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/450544/virtual-servers https://docs.fortinet.com/document/fortinac-f/7.6.0/fortiap-integration/445346/802-1x

1.5.11.15	Deve implementar, no mínimo, a autenticação para acesso dos usuários as redes WLAN e LAN utilizando MAC Address, 802.1x em base Local, Captive Portal e 802.1x em base externa.	FortiNAC-F 7.6.0 Administration Guide RADIUS Content editor Configure Local Server	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/214558/radius https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/512838/content-editor https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/463215/configure-local-server
1.5.11.16	Deve implementar autenticação RADIUS baseada em endereço MAC (Radius-based MAC authentication) dos dispositivos clientes.	FortiNAC-F 7.6.0 Administration Guide RADIUS Content editorConfigure Local Server	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/214558/radius https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/463215/configure-local-server
1.5.11.17	Deve implementar base de dados interna centralizada para registro dos endereços MAC dos dispositivos que serão autenticados por esta funcionalidade.	FortiNAC-F 7.6.0 Administration Guide Hosts / User/Host Management	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/487466/hosts https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/465615/user-host-management
1.5.11.18	Deve subdividir a base de MAC dos dispositivos em grupos para granularidade de acesso.	FortiNAC-F 7.6.0 Administration Guide Hosts / User/Host Management	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/487466/hosts https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/465615/user-host-management
1.5.11.19	A partir de um único ponto de cadastramento, deve permitir a carga de um arquivo contendo uma lista de endereços MAC permitidos ou a inclusão de uma lista de MAC's em um único campo como uma lista.	FortiNAC-F 7.6.0 Administration Guide Import and export data hosts	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/675602/import-and-export-data https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/487466/hosts
1.5.11.20	Deve implementar autenticação via portal web (captive portal) para os usuários da rede que não puderem se autenticar via 802.1x:	FortiNAC-F 7.6.0 Administration Guide Portal configuration Configure authentication credentials	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/600281/portal-configuration https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/654272/configure-authentication-credentials
a)	O serviço web de autenticação (captive portal) deve ser fornecido e hospedado dentro da solução ofertada, além de permitir que as requisições possam ser redirecionadas para um serviço externo;	FortiNAC-F 7.6.0 Administration Guide Portal configuration	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/600281/portal-configuration
b)	Para as redes abertas/guest vlan, utilizadas em eventos e para visitantes, o cliente deverá se conectar sem senha à infraestrutura de rede e ter seu acesso redirecionado para o portal de autenticação;	FortiNAC-F 7.6.0 Administration Guide Portal configuration Configure authentication credentials	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/600281/portal-configuration https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/654272/configure-authentication-credentials

c)	A autenticação de visitantes poderá ser realizada por login e senhas pré-cadastradas pela DPMG para cada indivíduo ou grupo. A autenticação de visitantes também poderá ser realizada mediante login e senha do usuário, em pelo menos, uma das seguintes redes sociais e serviços de e-mail públicos: GOV.BR, GMAIL/Google, Facebook, LinkedIn ou serviço que utilize o padrão OAuth 2.0 (RFC 6750 e 8252), de forma nativa ou via API;	FortiNAC-F 7.6.0 Administration Guide Guest & Contractor templates Social Media for Captive Portal	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/590109/guest-contractor-users https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/630619/social-media-for-captive-portal
d)	O captive portal deve ser suportado, no mínimo, pelos um dos seguintes navegadores de Internet: Microsoft Edge, Mozilla Firefox, Opera, Safari e Chrome; operando em PCs e dispositivos móveis;	FortiNAC-F 7.6.0 Web Browsers for the Administration UI	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/release-notes/38733
e)	Deve permitir a customização das páginas web do portal, com a inclusão de imagens, instruções em texto e campos de texto que devem ser preenchidos pelos clientes;	FortiNAC-F 7.6.0 Administration Guide Portal configuration	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/600281/portal-configuration
f)	Deve possuir suporte ao idioma Português.	FortiNAC-F 7.6.0 Administration Guide Portal configuration	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/600281/portal-configuration
1.5.11.21	Deve suportar diferentes grupos de servidores AAA (Authentication, Authorization and Accounting) de retaguarda ("Backend Authentication Servers"), como RADIUS, LDAP e Microsoft Active Directory (sem alteração no Schema do AD), Azure AD, Microsoft Entra ID, Base SQL Interna, HTTP, Lista estática de endereços MAC.	FortiNAC-F 7.6.0 Administration Guide using-windows-domain-logon-credentials directories global configure-authentication-credentials	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/60485/using-windows-domain-logon-credentials https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/982839/directories https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/505365/global https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/654272/configure-authentication-credentials
1.5.11.22	Implementar a arquitetura AAA (Authentication, Authorization e Accounting) para os clientes da rede.	FortiNAC-F 7.6.0 Administration Guide RADIUS	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/214558/radius
1.5.11.23	Implementar autenticação via servidor RADIUS Authentication (RFC 2865), Accounting (RFC 2866), Extensions (RFC 2869) ou TACACS (RFC 1492).	FortiNAC-F 7.6.0 Administration Guide Supported RFCs	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/supported-rfcs
1.5.11.24	Deve implementar atribuição dinâmica de ACL (Access Control Lists), QoS e VLAN, com base nos parâmetros da etapa de autenticação:	FortiNAC-F 7.6.0 Administration Guide Logical networks Assigning access values and CLI configurations	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/867742/logical-networks https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/519880/assigning-access-values-and-cli-configurations

a)	Esta atribuição dinâmica deve ocorrer em APs (para o tráfego de comutação local) e switches;	FortiNAC-F 7.6.0 Administration Guide Logical networks Assigning access values and CLI configurations Network access Attribute Groups	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/867742/logical-networks https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/519880/assigning-access-values-and-cli-configurations https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/926300/network-access https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/239599/attribute-groups
b)	Esta atribuição dinâmica deve ocorrer nos Controladores WLAN para redes com comutação central;	FortiNAC-F 7.6.0 Administration Guide Logical networks Assigning access values and CLI configurations	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/867742/logical-networks https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/519880/assigning-access-values-and-cli-configurations
c)	Deve suportar a criação de pelo menos 64 ACL's através dos equipamentos gerenciados desde que os mesmos suportem, cada uma com pelo menos 64 (sessenta e quatro) regras/linhas baseadas em endereços IP, protocolos e portas.	FortiNAC-F 7.6.0 Administration Guide Attribute Groups	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/239599/attribute-groups
1.5.11.25	Deve implementar o protocolo RADIUS Change of Authorization (CoA) conforme a RFC 5176 ou RFC 3576.	FortiNAC-F 7.6.0 Administration Guide FortiNAC- Supported RFCs Overview RADIUS	LINK / PG15	https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/0ffca6b5-75e1-11ef-8355-fa163e15d75b/FortiNAC-F_7.x-supported-rfcs-pdf.pdf https://docs.fortinet.com/document/fortinac-f/7.6.0/rfc5176-coa-disconnect-message/562583/overview https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/214558/radius
1.5.11.26	Deve possuir ferramenta, portal de autosserviço, para gerenciar os processos de credenciamento, autenticação, autorização e contabilidade de usuários visitantes através de um portal web seguro:	FortiNAC-F 7.6.0 Administration Guide Guest self registration Portal page setup Portal configuration	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/687558/guest-self-registration https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/5279/portal-page-setup https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/600281/portal-configuration
a)	Deve implementar a criação de grupos de autorizadores com privilégios de criação de credenciais temporárias e atribuição de permissões de acesso aos clientes;	FortiNAC-F 7.6.0 Administration Guide Administrator profile	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/752345/administrator-profile
b)	Deve realizar a autenticação dos autorizadores em base externa do tipo Microsoft Active Directory ou LDAP e atribuir o privilégio ao autorizador de acordo com o seu perfil;	FortiNAC-F 7.6.0 Administration Guide Configure authentication credentials	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/654272/configure-authentication-credentials
c)	Deve implementar as funcionalidades de geração aleatória de lotes de credenciais temporárias pré autorizadas;	FortiNAC-F 7.6.0 Administration Guide Add a guest manager profile	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/300172/add-a-guest-manager-profile

d)	Deve implementar a importação e exportação da relação de credenciais temporárias através de arquivos txt ou csv;	FortiNAC-F 7.6.0 Administration Guide Import and export data	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/675602/import-and-export-data
e)	Deve permitir a criação de perfis de acesso para as credenciais temporárias com diferentes privilégios de acesso à rede;	FortiNAC-F 7.6.0 Administration Guide Guest & Contractor templates	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/145401/guest-contractor-templates
f)	Deve permitir a criação de perfis de validade das credenciais, baseando o início da validade na criação da conta ou no primeiro login da conta;	FortiNAC-F 7.6.0 Administration Guide Guest account details Account activation Guest & Contractor templates Guest & Contractor users Add a guest manager profile Guest self registration	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/945705/guest-account-details https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/747272/account-activation https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/145401/guest-contractor-templates https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/590109/guest-contractor-users https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/300172/add-a-guest-manager-profile https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/687558/guest-self-registration
g)	Deve permitir que o visitante crie sua própria credencial temporária (“self-service”) através do portal web, sem a necessidade de um autorizador com envio dos dados de acesso;	FortiNAC-F 7.6.0 Administration Guide Guest self registration	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/687558/guest-self-registration
h)	Deve permitir a customização do formulário de criação de credenciais, a ser preenchido pelo autorizador, especificando quais informações cadastrais dos visitantes são obrigatórias ou opcionais e permitindo criar campos novos ou possuir, minimamente, os seguintes campos pré- definidos: login/guest name; senha; nome completo/full name; email; telefone; empresa e outros campos que permitam colocar um texto e o número dos documentos de identificação do visitante;	FortiNAC-F 7.6.0 Administration Guide Guest & Contractor users Portal page setup Registration	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/590109/guest-contractor-users https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/5279/portal-page-setup https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/628079/registration
i)	Deve permitir a customização do nível de segurança da senha temporária que será gerada ao visitante, especificando a quantidade mínima de caracteres e o uso de caracteres especiais e números para compor a senha.	FortiNAC-F 7.6.0 Administration Guide Guest & Contractor users Portal page setup Registration	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/590109/guest-contractor-users https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/5279/portal-page-setup https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/628079/registration

1.5.11.27	Deve permitir a troca da senha pelo próprio visitante diretamente no portal web (captive portal);	FortiNAC-F 7.6.0 Administration Guide Guest self registration Social Media for Captive Portal Global Rest API	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/687558/guest-self-registration https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/630619/social-media-for-captive-portal https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/505365/global https://docs.fortinet.com/document/fortinac-f/7.6.3/rest-api/390805/introduction
1.5.11.28	Deve exigir que o usuário visitante aceite o “Termo de uso da rede” a cada login ou apenas no primeiro login.	FortiNAC-F 7.6.0 Administration Guide Registration	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/628079/registration
1.5.11.29	Deve implementar o envio das credenciais aos usuários registrados através de mensagens SMS (Short Message Service) ou email.	FortiNAC-F 7.6.0 Administration Guide Send Message	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/500807/send-message
1.5.11.30	Deve implementar funcionalidades de Classificação Automática de Dispositivos (“Device profiling”), de forma a descobrir, classificar e agrupar os dispositivos conectados na rede, permitindo extrair informações de contexto que devem ser usadas na aplicação de políticas de acesso.	FortiNAC-F 7.6.0 Administration Guide Profiled devices	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/316243/profiled-devices
1.5.11.31	Deve possuir interface gráfica para construção de regras e categorias customizadas de classificação de dispositivos.	FortiNAC-F 7.6.0 Administration Guide Menus	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/59799/menus
1.5.11.32	Deve permitir que o administrador cadastre manualmente um determinado dispositivo em uma categoria.	FortiNAC-F 7.6.0 Administration Guide Device profiling rules Menus	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/510340/device-profiling-rules https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/59799/menus
1.5.11.33	Deve possuir base de regras e categorias de dispositivos pré-configurada.	FortiNAC-F 7.6.0 Administration Guide Grupos	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/81184/groups
1.5.11.34	Deve suportar mecanismo de atualização das regras e categorias pré-configuradas.	FortiNAC-F 7.6.0 Administration Guide Updates Device Profiler	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/108094/updates https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/855329/device-profiler
1.5.11.35	Deve implementar gerenciamento e aplicação de políticas de autorização de acesso de usuários com base em:			
a)	Atributos LDAP do usuário autenticado;	FortiNAC-F 7.6.0 Administration Guide Policy & Objects Configure authentication credentials	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/323706/policy-objects https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/654272/configure-authentication-credentials
b)	Grupo do usuário no Active Directory;			
c)	Hora do dia, dia da semana;			
d)	Tipo de dispositivo utilizado;			
e)	Informações sobre o dispositivo utilizado (chave de registro, versão de SO, etc.);			
f)	Localização do usuário (dispositivo da rede de onde partiu a tentativa de acesso);			
g)	Tipo de autenticação utilizada.			

1.5.11.36	Deve implementar funcionalidades de avaliação de postura de segurança (NAC/NAP) nos dispositivos clientes.	FortiNAC-F 7.6.0 Administration Guide Scans	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/4612/scans
1.5.11.37	Deve permitir a Avaliação de Postura de Segurança através de Agente instalado permanente, compatível com os sistemas operacionais Microsoft Windows 10 ou superior, Apple MacOS e Linux Ubuntu ou Agente temporário compatível com os navegadores Microsoft Edge, Mozilla Firefox e Chrome, executados no Microsoft Windows 10 ou superior e Apple MacOS.	FortiNAC-F 7.6.0 Administration Guide Dissolvable Agent Persistent Agent	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/143138/persistent-agent https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/878424/dissolvable-agent
1.5.11.38	A plataforma em conjunto com o agente deve impedir que o usuário desative, remova ou altere as configurações do agente. Além disso, a aplicação dessas restrições deve ser possível de ser realizada por meio de diretivas de grupo (GPO).	FortiNAC-F 7.6.0 Administration Guide Administrative templates for GPO Persistent Agent	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/941268/administrative-templates-for-gpo https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/143138/persistent-agent
1.5.11.39	Os agentes devem permitir a verificação dos seguintes itens: atualizações do sistema operacional, estado e atualizações dos softwares de firewall, antivírus, antispymware. No mínimo, os seguintes fabricantes de antivírus e SO deverão ser suportados: SO – Microsoft (Windows 10 ou superior) e Apple (MacOS); AV Symantec, Microsoft, McAfee e Kaspersky.	FortiNAC-F 7.6.0 Administration Guide Agent updates Endpoint compliance policies for guests	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/682958/endpoint-compliance-policies-for-guests https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/40687/agent-updates
1.5.11.40	Deve implementar mecanismo de isolamento ou quarentena dos dispositivos que estiverem em desacordo com as políticas de segurança. Caso o dispositivo do usuário não esteja de acordo com as políticas de segurança, a solução deverá prover mecanismo de remediação que permita ao usuário atualizar seu dispositivo.	FortiNAC-F 7.6.0 Administration Guide Remediation Control	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/120935/remediation https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/280568/control
1.5.11.41	Deve implementar relatórios com as informações referentes aos resultados da verificação de postura dos dispositivos clientes.	FortiNAC-F 7.6.0 Administration Guide Scans View logs and reports Reports	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/4612/scans https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/238560/view-logs-and-reports https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/521642/reports
1.5.11.42	Deve implementar funcionalidades de provisionamento automático (Onboarding) das configurações 802.1x para os dispositivos clientes com sistemas Windows 10 ou superior, Apple iOS, Apple MacOS e Android.	FortiNAC-F 7.6.0 Administration Guide SSID mappings	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/456273/ssid-mappings
1.5.11.43	Deve implementar/estar licenciado os serviços de autenticação, profiling, provisionamento e autorização para 1.000 (mil) usuários simultâneos ou 1.000 (mil) dispositivos simultâneos.	FortiNAC-F 7.6.0 Administration Guide License Information	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/304993/license-information

1.5.11.44	Deve ser fornecida com todos os recursos necessários para implementar mecanismo de alta disponibilidade para as funções de Autenticação/portal e Autorização/NAC, utilizando componentes redundantes em modo ativo-passivo ou ativo-ativo. Cada componente deverá suportar, individualmente, todo o volume de uso especificado.	FortiNAC-F 7.6.0 Administration Guide High availability concepts	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/300084/high-availability-concepts
1.5.11.45	Deve implementar "Single Sign-on" (SSO) através de SAML v2.0.	FortiNAC-F 7.6.0 Administration Guide Overview	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.3/saml-ssso/512695/overview
1.5.11.46	Permitir a visualização de todas informações relativas a cada transação/autenticação em uma única tela, como Data e Hora, Mac Address do dispositivo, classificação do dispositivo, Usuário, equipamento que requisitou a autenticação (origem), Método de autenticação utilizado, fonte de autenticação utilizada para validação, perfil de acesso aplicado, todos atributos de entrada do protocolo utilizados na requisição (ex. RADIUS), informações de resposta da solução para o elemento de rede, alertas em caso de falha, e exibição dos Log já filtrados para a requisição em análise.	FortiNAC-F 7.6.0 Administration Guide RADIUS Authentication	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/fortiap-integration/312789/radius-authentication
1.5.11.47	Deve possuir Dashboard customizável, onde deve permitir a visualização de no mínimo as seguintes informações:	FortiNAC-F 7.6.0 Administration Guide Dashboard RADIUS Activity Adding widgets	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/964529/dashboard https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/457521/radius-activity https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/333483/adding-widgets
a)	Lista com os últimos Alertas do sistema;			
b)	Gráfico com todas as requisições de autenticação dos últimos 7 (sete) dias, incluindo RADIUS e Web Authentication;			
c)	Gráfico com o status das autenticações aceitas e rejeitadas nos últimos 7 (sete) dias;			
d)	Para soluções compostas por mais de um servidor/appliance, deve apresentar o Status de cada elemento dos sistemas, com informações como endereço IP e data da última replicação dos dados;			
e)	Gráfico com a categorização dos dispositivos classificados pela solução, divididos de acordo com as categorias de classificação;			
f)	Últimas falhas de autenticação;			
g)	Lista com as últimas autenticações com sucesso;			
h)	Utilização de CPU do sistema, no mínimo nos últimos 30 (trinta) minutos.			
1.5.11.48	Deve implementar a coleta de informações, para classificação, usando no mínimo DHCP, HTTP User-Agent, MAC OUI, ActiveSync plugin, SNMP, Subnet Scanner, IF-MAP, Cisco Device Sensor, MDM e TCP Fingerprinting.	FortiNAC-F 7.6.0 Administration Guide Device profiling rules	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/510340/device-profiling-rules
1.5.11.49	Deve implementar no mínimo os seguintes métodos de autenticação:			

a)	EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS);	FortiNAC-F 7.6.0 Administration Guide Configure Local RADIUS Server settings	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/366458/configure-local-radius-server-settings
b)	PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public, EAP-PWD);			
c)	TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, PAP, CHAP);			
d)	EAP-TLS;			
e)	PAP, CHAP, MSCHAPv1, MSCHAPv2, and EAP-MD5;			
f)	Windows machine authentication;			
g)	SMB v2/v3;			
h)	WPA3 – MPSPK;			
i)	RADSec;			
j)	Online Certificate Status Protocol (OCSP);			
k)	WEB Authentication.			
1.5.11.50	Deve suportar a verificação de vulnerabilidade através de varredura de portas (NMAP).	FortiNAC-F 7.6.0 Administration Guide Device profiler	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/855329/device-profiler
1.5.11.51	Suporte a aplicação de políticas em ambiente multivendor de Wireless, cabeado e VPN.	FortiNAC-F 7.6.0 Administration Guide Policy assignment Policy & Objects Portal policy Policies	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/49701/policy-assignment https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/323706/policy-objects https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/567487/portal-policy https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/985922/policies
1.5.11.52	Deve suportar integração com no mínimo Brocade, Palo Alto, Splunk, Juniper, Fortinet e Check Point, ServiceNow, McAfee, Twilio.	FortiNAC Device Integration Guides Third Party Ecosystem Integration FortiNAC-F Datasheet Third Party Ecosystem Integration FortiNAC-F 7.6.3 Rest API	Link / PG 06	https://docs.fortinet.com/document/fortinac-f/7.6.0/device-integration-guides/781318/fortinac-device-integration-guides https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortinac.pdf https://docs.fortinet.com/document/fortinac-f/7.6.3/rest-api/390805/introduction
1.5.11.53	Deve permitir configurar um meio para proteger a comunicação entre clientes RADIUS / TCP na camada de transporte, utilizando TLS para encriptação da comunicação.	FortiNAC-F 7.6.0 Administration Guide FortiNAC Access Configuration	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/193428/fortinac-access-configuration
1.5.11.54	Suporte à integração com plataforma de terceiros usando HTTP/RESTful API.	FortiNAC-F 7.6.0 Administration Guide Welcome to the FortiNAC REST API!	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/rest-api/390805/introduction
1.5.11.55	Permitir que a solução faça consultas em bases SQL, com o objetivo de buscar informação a serem utilizadas durante o processo de autenticação dos usuários.	FortiNAC-F 7.6.3 Rest API	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.3/rest-api/390805/introduction
1.5.11.56	Suporte aos seguintes recursos através de IPv6:			
a)	Administração via WEB e CLI;	FortiNAC-F 7.6.0 Administration Guide IPv6 support	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/168784/ipv6-support
b)	Servidores de autenticação e autorização com endereçamento IPv6;			
c)	IPv6 Accounting Proxy;			
d)	Acesso a servidores com endereçamento IPv6 para contexto de endpoints;			
e)	Syslog, DNS, NTP;			

f)	Endereçamento IPv6 para VIP (Virtual IP) de alta disponibilidade;			
g)	Fontes de Syslog para processamento de eventos;			
1.5.11.57	Fontes de Syslog para processamento de eventos;fips			
a)	FIPS 140-2;	FortiNAC-F 7.6.0 Federal Information Processing Standards Fortinet Community Knowledge Base Network Security	LINK	https://www.fortinet.com/corporate/about-us/product-certifications/fips https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4497 https://community.fortinet.com/fortigate-3/technical-tip-fortios-fips-resource-list-192150 https://community.fortinet.com/fortigate-3/technical-tip-extended-support-for-v7-0-fips-cc-certified-cve-patched-firmware-212653 https://community.fortinet.com/fortigate-3/technical-tip-key-considerations-when-upgrading-fips-fortigates-from-fips-140-2-v7-0-and-earlier-to-fips-140-3-v7-2-v7-4-and-later-222013
b)	Common Criteria NDCPP + Servidor de autenticação;	FortiNAC-F 7.6.0 Administration Guide Common Criteria	LINK	https://www.fortinet.com/br/corporate/about-us/product-certifications/common-criteria https://www.niap-ccevs.org/products/11562 https://www.commoncriteriaportal.org/products/index.cfm
1.5.11.58	A solução deve permitir configuração em alta disponibilidade com no mínimo dois elementos, sendo que ambos devem permanecer ativos para o processamento das requisições.	FortiNAC-F 7.6.0 High Availability (FortiNAC-OS)	LINK	Overview FortiNAC-F 7.6.0 Fortinet Document Library
1.5.11.59	A solução deve permitir a configuração centralizada de políticas em ambientes distribuídos, no qual as políticas serão configuradas em um único elemento para serem distribuídas aos demais que pertençam a mesma "zona".	FortiNAC-F 7.6.0 Administration Guide FortiNAC Manager	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/991647/fortinac-manager
1.5.11.60	A solução deve permitir a geração e o envio através de e-mail ou SMS de alertas relativos as seguintes atividades anormais detectadas na rede:			
a)	Autenticações;	FortiNAC-F 7.6.0 Administration Guide Bulk modify alarm mappings	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/33938/bulk-modify-alarm-mappings
b)	Acesso a dispositivos de rede;			
c)	Tentativa de execução de comandos em dispositivos de rede por usuários sem privilégios;			
d)	Atividades irregulares nos servidores da solução;			

1.5.11.61	A solução deve possuir ferramenta para geração de relatórios de maneira centralizada, permitindo o agendamento e envio por e mail em formato HTML e PDF.	FortiNAC-F 7.6.0 Administration Guide View logs and reports Reports Preview a custom report Schedule reports	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/238560/view-logs-and-reports https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/521642/reports https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/930556/preview-a-custom-report https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/164999/schedule-reports
1.5.11.62	Deve contemplar suporte do fabricante por 5 (cinco) anos:	DE ACORDO COM A PROPOSTA COMERCIAL		
	a) Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais;	DE ACORDO COM A PROPOSTA COMERCIAL DE ACORDO COM A PROPOSTA TÉCNICA		https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/108094/updates https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/90778/licenses
	b) Suporte telefônico para abertura de chamados em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito disponibilizado pelo fabricante. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos.	DE ACORDO COM A PROPOSTA COMERCIAL DE ACORDO COM A PROPOSTA TÉCNICA		https://www.fortinet.com/br/support
1.5.11.63	Funcionalidades para autenticação de usuários visitantes:			
a)	A solução de controle de acesso deve implementar funcionalidades para autenticação de usuários visitantes;	FortiNAC-F 7.6.0 Administration Guide Captive Portal Configuration Open SSID for guest management	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/rest-api/108175/captive-portal-configuration https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/219021/open-ssid-for-guest-management
b)	Deve implementar funcionalidade para gerenciar os processos de credenciamento, autenticação, autorização e contabilidade de usuários visitantes através de um portal web seguro;	FortiNAC-F 7.6.0 Administration Guide Captive Portal Configuration Open SSID for guest management	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/rest-api/108175/captive-portal-configuration https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/219021/open-ssid-for-guest-management
c)	Deve implementar a criação de grupos de autorizadores com privilégios distintos, por SSID, de criação de credenciais temporárias e atribuição de permissões de acesso aos clientes;	FortiNAC-F 7.6.0 Administration Guide Captive Portal Configuration Open SSID for guest management	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/rest-api/108175/captive-portal-configuration https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/219021/open-ssid-for-guest-management
d)	Deve implementar a autenticação dos autorizadores em base externa do tipo Microsoft Active Directory ou LDAP e atribuir o privilégio ao autorizador de acordo com o seu perfil;	FortiNAC-F 7.6.0 Administration Guide Captive Portal Configuration Open SSID for guest management	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/rest-api/108175/captive-portal-configuration https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/219021/open-ssid-for-guest-management

e)	Deve suportar as funcionalidades de geração aleatória de lotes de credenciais temporárias pré-autorizadas;	FortiNAC-F 7.6.0 Administration Guide Captive Portal Configuration Open SSID for guest management	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/rest-api/108175/captive-portal-configuration https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/219021/open-ssid-for-guest-management
f)	Deve suportar a importação e exportação da relação de credenciais temporárias através de arquivos txt ou csv;	FortiNAC-F 7.6.0 Administration Guide Captive Portal Configuration Open SSID for guest management	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/rest-api/108175/captive-portal-configuration https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/219021/open-ssid-for-guest-management
g)	Deve implementar a criação de validade das credenciais, baseando o início da validade na criação da conta ou no primeiro login da conta;	FortiNAC-F 7.6.0 Administration Guide Captive Portal Configuration Open SSID for guest management	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/rest-api/108175/captive-portal-configuration https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/219021/open-ssid-for-guest-management
h)	Deve implementar que o visitante crie sua própria credencial temporária ("self-service") através do portal web, sem a necessidade de um autorizador;	FortiNAC-F 7.6.0 Administration Guide Captive Portal Configuration Open SSID for guest management	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/rest-api/108175/captive-portal-configuration https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/219021/open-ssid-for-guest-management
i)	Deve implementar a customização do formulário de criação de credenciais, a ser preenchido pelo autorizador ou pelo visitante, em caso de auto-serviço, especificando quais informações cadastrais dos visitantes são obrigatórias ou opcionais;	FortiNAC-F 7.6.0 Administration Guide Captive Portal Configuration Open SSID for guest management	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/rest-api/108175/captive-portal-configuration https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/219021/open-ssid-for-guest-management
j)	Deve implementar a customização do nível de segurança da senha temporária que será gerada ao visitante, especificando a quantidade mínima de caracteres e o uso de caracteres especiais e números para compor a senha;	FortiNAC-F 7.6.0 Administration Guide Captive Portal Configuration Open SSID for guest management	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/rest-api/108175/captive-portal-configuration https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/219021/open-ssid-for-guest-management
k)	Deve exigir que o usuário visitante aceite o "Termo de uso da rede" a cada login ou apenas no primeiro login;	FortiNAC-F 7.6.0 Administration Guide Captive Portal Configuration Open SSID for guest management	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/rest-api/108175/captive-portal-configuration https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/219021/open-ssid-for-guest-management
l)	Deve suportar o envio das credenciais aos usuários registrados através de mensagens SMS (Short Message Service), email e impressão local;	FortiNAC-F 7.6.0 Administration Guide Captive Portal Configuration Open SSID for guest management	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/rest-api/108175/captive-portal-configuration https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/219021/open-ssid-for-guest-management
m)	Deve implementar que a customização da página de registro de visitantes para campos relacionados a confirmação de sponsorship;	FortiNAC-F 7.6.0 Administration Guide Captive Portal Configuration Open SSID for guest management	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/rest-api/108175/captive-portal-configuration https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/219021/open-ssid-for-guest-management

n)	Deve implementar o gerenciamento das credenciais de visitantes;	FortiNAC-F 7.6.0 Administration Guide Captive Portal Configuration Open SSID for guest management	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/rest-api/108175/captive-portal-configuration https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/219021/open-ssid-for-guest-management
o)	Deve implementar a configuração de contas de usuários visitantes com as seguintes características: Prazo de validade, largura de banda;	FortiNAC-F 7.6.0 Administration Guide Captive Portal Configuration Open SSID for guest management	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/rest-api/108175/captive-portal-configuration https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/219021/open-ssid-for-guest-management
p)	Deve implementar o caching de endereço MAC dos usuários visitantes;	FortiNAC-F 7.6.0 Administration Guide Captive Portal Configuration Open SSID for guest management	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/rest-api/108175/captive-portal-configuration https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/219021/open-ssid-for-guest-management
q)	Deve suportar o login automático de usuários que realizem o auto-registro;	FortiNAC-F 7.6.0 Administration Guide Captive Portal Configuration Open SSID for guest management	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/rest-api/108175/captive-portal-configuration https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/219021/open-ssid-for-guest-management
r)	Deve suportar a autenticação de usuário anônimo sem necessidade de prover usuário e senha;	FortiNAC-F 7.6.0 Administration Guide Captive Portal Configuration Open SSID for guest management	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/rest-api/108175/captive-portal-configuration https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/219021/open-ssid-for-guest-management
s)	Deve suportar a criação de token de acesso;	FortiNAC-F 7.6.0 Administration Guide Captive Portal Configuration Open SSID for guest management	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/rest-api/108175/captive-portal-configuration https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/219021/open-ssid-for-guest-management
t)	Deve suportar a criação e gerenciamento de múltiplas contas de usuários visitantes;	FortiNAC-F 7.6.0 Administration Guide Captive Portal Configuration Open SSID for guest management	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/rest-api/108175/captive-portal-configuration https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/219021/open-ssid-for-guest-management
u)	Deve implementar a desconexão de múltiplas sessões ativas;	FortiNAC-F 7.6.0 Administration Guide Captive Portal Configuration Open SSID for guest management	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/rest-api/108175/captive-portal-configuration https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/219021/open-ssid-for-guest-management
v)	Deve suportar página que exibe estatística de sessão após realizar login para que os usuários possam monitorar sua utilização e cota atribuída;	FortiNAC-F 7.6.0 Administration Guide Captive Portal Configuration Open SSID for guest management	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/rest-api/108175/captive-portal-configuration https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/219021/open-ssid-for-guest-management

w)	Deve implementar autenticação através de social login nativa na solução;	FortiNAC-F 7.6.0 Administration Guide Captive Portal Configuration Open SSID for guest management	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/rest-api/108175/captive-portal-configuration https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/219021/open-ssid-for-guest-management
x)	Deve implementar a capacidade de modificar ou desconectar uma sessão ativa de visitante através de RADIUS Dynamic Authorization.	FortiNAC-F 7.6.0 Administration Guide Captive Portal Configuration Open SSID for guest management	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/rest-api/108175/captive-portal-configuration https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/219021/open-ssid-for-guest-management
1.5.11.64	Funcionalidade de análise dispositivo de acesso:			
	a) Deve suportar funcionalidade para verificação das políticas de segurança implementadas nos dispositivos conectados à rede, através de agentes instalados ou temporários.	FortiNAC-F 7.6.0 Administration Guide Captive Portal Configuration Agents	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/release-notes/319593/agents
1.5.11.65	Permitir a execução do agente como serviço quando instalado em sistemas Windows;.			
	a) Permitir o uso de agentes instalados nos dispositivos, ou agente temporários para o uso em dispositivos de terceiros que necessitem acesso à rede;	FortiNAC-F 7.6.0 Administration Guide Installation for Windows	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/186057/installation-for-windows
	b) Permitir o gerenciamento centralizado das políticas, e permitir que os usuários/dispositivos que estiverem fora das políticas de segurança, sejam direcionados para um segmento de rede específico ou determinação de uma política de acesso restritiva, permitindo ainda que estes consigam se adequar a respectiva política (remediação);	FortiNAC-F 7.6.0 Administration Guide Remediation configurations	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/445618/remediation-configurations
	c) Permitir que a solução realize a adequação da política (remediação) de forma automática, sem necessidade de intervenção do usuário;	FortiNAC-F 7.6.0 Administration Guide Remediation configurations	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/445618/remediation-configurations
1.5.11.66	Deve suportar a verificação de pelos menos os seguintes serviços:			
a)	Firewall;	FortiNAC-F 7.6.0 Administration Guide Endpoint Compliance	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/fortinac-deployment-guide/667802/endpoint-compliance
b)	Conexões de rede;	FortiNAC-F 7.6.0 Administration Guide Scans	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/4612/scans
c)	Windows Hotfixes;	FortiNAC-F 7.6.0 Administration Guide Endpoint Compliance	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/fortinac-deployment-guide/667802/endpoint-compliance
d)	Máquinas Virtuais;	FortiNAC-F 7.6.0 Administration Guide Scans	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/4612/scans
e)	Aplicações instaladas;	FortiNAC-F 7.6.0 Administration Guide Scans	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/4612/scans
f)	Serviços;	FortiNAC-F 7.6.0 Administration Guide Scans	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/4612/scans
g)	Dispositivos USB;	FortiNAC-F 7.6.0 Administration Guide Scans	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/4612/scans

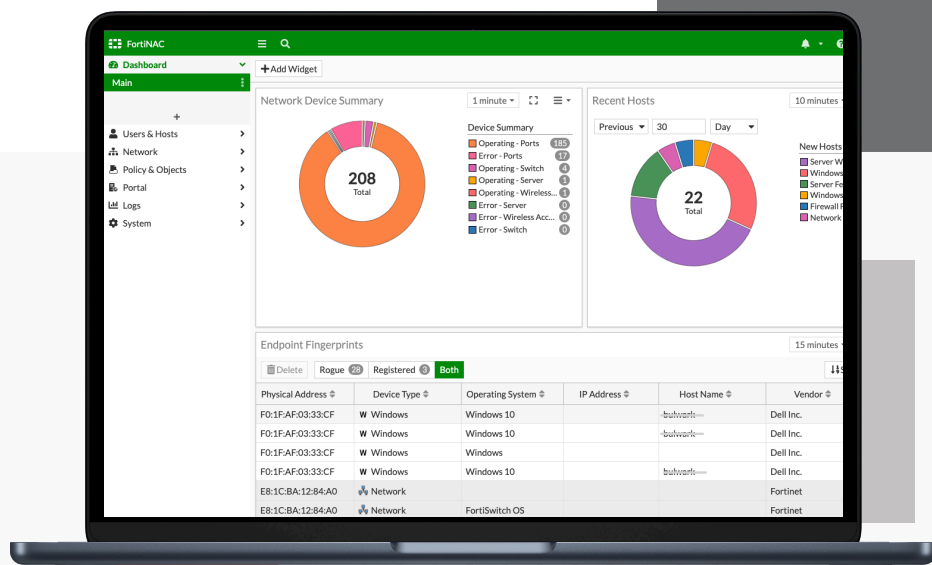
h)	Processos;	FortiNAC-F 7.6.0 Administration Guide Scans	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/4612/scans
i)	Checação de arquivos;	FortiNAC-F 7.6.0 Administration Guide Scans	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/4612/scans
j)	Criptografia de disco;	FortiNAC-F 7.6.0 Administration Guide Endpoint Compliance	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/fortinac-deployment-guide/667802/endpoint-compliance
k)	Aplicações peer to peer.	FortiNAC-F 7.6.0 Administration Guide Endpoint Compliance	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/fortinac-deployment-guide/667802/endpoint-compliance
1.5.11.67	Deve suportar a verificação de Anti-virus com pelos menos os seguintes parâmetros:			
	a) Produto instalado;	FortiNAC-F 7.6.0 Administration Guide Endpoint Compliance	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/143138/persistent-agent
	b) Versão instalada;			
	c) Data da última atualização;			
	d) Data da última verificação;			
1.5.11.68	A plataforma deve suportar a integração com SCCM, ou Intune ou WSUS.	FortiNAC-F 7.6.0 Administration Guide Operating system parameters - Windows MDM Servers	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/422594/mdm-servers https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/993701/operating-system-parameters-windows
1.5.11.69	Deve permitir a verificação de postura de dispositivos Windows 10/11 sem a necessidade de instalação prévia de agentes, executando todas as operações de verificação em "background", ou seja, transparente ao usuário final.	FortiNAC-F 7.6.0 Administration Guide Run the agentless scanner	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/570585/run-the-agentless-scanner
1.5.11.70	Funcionalidade de provisionamento dispositivo de acesso:			
a)	Implementar a Autoridade Certificadora (CA) integrada para uso no provisionamento de dispositivos pessoais (BYOD);	FortiNAC-F 7.6.0 Administration Guide Certificate management	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/454803/certificate-management
b)	Deve implementar funcionalidades de provisionamento automático (Onboarding) de configurações 802.1x;	FortiNAC-F 7.6.0 Administration Guide Secure SSID for device onboarding	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/549892/secure-ssid-for-device-onboarding
c)	Suporte ao provisionamento automático de dispositivos, através de Portal Captivo para Windows, Mac OSX, iOS, Android, Chromebook e Linux Ubuntu;	FortiNAC-F 7.6.0 Administration Guide Portal configuration	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/600281/portal-configuration
d)	Deve implementar configurações, no mínimo, de EAP-TLS e EAP-PEAP;	FortiNAC-F 7.6.0 Administration Guide Configure Local Server Configure Local RADIUS Server settings	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/366458/configure-local-radius-server-settings https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/463215/configure-local-server
e)	Deve suportar a configuração de servidor endereço IP e porta de proxy para os dispositivos móveis IOS, Android e macOS 10.7 e posteriores;	FortiNAC-F 7.6.0 Administration Guide Portal configuration	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/600281/portal-configuration

f)	Deve suportar portal de auto-serviço (self-service) que permita que os usuários finais possam registrar e remover dispositivos e reportar perda ou roubo de um dispositivo, sem a necessidade do envolvimento da equipe de TI;	FortiNAC-F 7.6.0 Administration Guide Portal configuration	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/600281/portal-configuration
g)	Deve implementar a geração e instalação de um certificado individual para cada dispositivo cliente;	FortiNAC-F 7.6.0 Administration Guide Certificate management	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/454803/certificate-management
h)	Deve implementar a revogação do certificado de um dispositivo específico, para caso de perda ou roubo;	FortiNAC-F 7.6.0 Administration Guide Certificate management	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/454803/certificate-management
i)	Deve implementar a verificação da validade dos certificados digitais através do protocolo OCSP (Online Certificate Status Protocol);	FortiNAC-F 7.6.0 Administration Guide Certificate management Configure Local RADIUS Server settings	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/454803/certificate-management https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/366458/configure-local-radius-server-settings
j)	Deve implementar utilização de um único SSID para o provisionamento e a conexão após provisionamento dos dispositivos, utilizando os métodos PEAP e EAP-TLS no mesmo SSID;	FortiNAC-F 7.6.0 Administration Guide Configure Local RADIUS Server settings Secure SSID for device onboarding	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/366458/configure-local-radius-server-settings https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/549892/secure-ssid-for-device-onboarding
k)	Deve possibilitar a visualização do número de certificados emitidos para cada sistema operacional de dispositivo;	FortiNAC-F 7.6.0 Administration Guide Certificate management	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/454803/certificate-management
l)	Deve controlar os usuários com permissão para provisionamento de novos dispositivos, através da autenticação utilizando o Active Directory e também a utilização de credenciais disponibilizadas por repositórios em nuvem;	FortiNAC-F 7.6.0 Administration Guide Portal configuration Configure Local Server	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/463215/configure-local-server https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/600281/portal-configuration
m)	Deve suportar a distribuição de certificados gerados a partir da solicitação de aplicações de terceiros como EMM/MDM utilizando para isso os protocolos SCEP e EST em conformidade com a RFC 7030.	FortiNAC-F 7.6.0 Administration Guide Server certificates	LINK	https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/691790/server-certificates
1.5.11.71	Instalação e Configuração:			

	a) As atividades de instalação/configuração da solução deverão ser realizadas dentro do horário comercial de segunda a sexta-feira, das 08:00 h às 18:00 h, nas dependências do Contratante, com posterior repasse de conhecimento das principais funcionalidades dos equipamentos, da solução e da configuração implementada, em formato hands on para a equipe técnica designada do Contratante, com carga horária mínima de 20 (vinte) horas.	DE ACORDO COM A PROPOSTA COMERCIAL DE ACORDO COM A PROPOSTA TÉCNICA		
1.5.12	LICENCA ADICIONAL DE SOLUCAO DE CONTROLE DE ACESSO A REDE (NAC) – ITEM 2 / LOTE 02			
1.5.12.1	Deve incrementar à solução de controle de acesso aos usuários e dispositivos os serviços de autenticação, profiling e autorização (ITEM 01 / LOTE 02) para 500 (quinhentos) usuários ou dispositivos simultaneamente;	DE ACORDO COM A PROPOSTA COMERCIAL DE ACORDO COM A PROPOSTA TÉCNICA		
1.5.12.2	Deve possuir suporte técnico e atualizações de software pelo fabricante de pelo menos 60 (sessenta) meses comprovado por declaração do fabricante ou fornecimento de PN do suporte técnico ofertado;	DE ACORDO COM A PROPOSTA COMERCIAL DE ACORDO COM A PROPOSTA TÉCNICA		
1.5.12.3	É obrigatório incluir na proposta a marca e o modelo específico do(s) equipamento(s) e/ou software(s) e demais componente(s) ofertado(s) para atendimento das especificações contidas nesse Termo de Referência.	DE ACORDO COM A PROPOSTA COMERCIAL DE ACORDO COM A PROPOSTA TÉCNICA		

FortiNAC

FortiNAC F Series Hardware, VM, and Endpoint Licenses



Highlights

- Discover and maintain an updated inventory of all network devices, including BYOD, IoT, OT, and IoMT
- Continuously assess risks for every endpoint using real-time threat intelligence and behavioral patterns
- Implement dynamic network scanning to classify and analyze device behaviors using continuous, automated techniques
- Expand Zero Trust to end devices with always-on identity checks and least privilege access
- Integrate with various third-party network tools ensuring compatibility
- Relay real-time contextual data to SIEM, improving incident response.

Visibility, Zero Trust Access, and Incident Response for Connected Assets and Users

FortiNAC continues to be a cutting-edge network access control solution, enabling organizations to enforce network access policies and assure adherence to security protocols in light of increasingly sophisticated threats. It provides a comprehensive snapshot of all devices and users on the network, facilitating granular control of access based on user roles, device types, network locations, and now enhanced with the behavioral patterns of devices and users.

The solution's capability now extends beyond automated onboarding of new endpoints; it incorporates real-time threat intelligence and continuous risk assessment of devices, leveraging machine learning and AI technologies from FortiGuard Services. Given the rising prominence of BYOD (Bring Your Own Device) and IoT (Internet of Things), the FortiNAC continuous monitoring and immediate remediation of non-compliant devices have become even more crucial.

Moreover, FortiNAC's integration goes beyond third-party networking and security solutions; it integrates with a wide range of cloud-based platforms and DevOps tools to ensure seamless and secure network operations in hybrid IT environments. FortiNAC leverages its integration with FortiAnalyzer to gain deep insight into network security posture, encompassing real-time visibility, predictive analytics, and more robust compliance reporting. Organizations can use FortiNAC to build a solid foundation for a secured network that can more effectively protect against unauthorized access, potential threats, and increasingly, the insider threats. The net result aligns with the emerging Zero Trust security model that emphasizes "never trust, always verify".

Features

Available in



Appliance



Virtual

Granular Visibility Across the Network for Every Device and User

FortiNAC leverages AI and machine learning from FortiGuard Security Services to provide detailed profiling of devices (FortiNAC native 27 categories + FortiGuard 133 categories), including headless devices and IoT assets on your network. This profiling incorporates multiple information sources, behavior patterns, and real-time threat intelligence to accurately identify and assess what is on your network.

Seamless Integration and Control Across Diverse Environments

With the power of micro-segmentation and Zero Trust policies, FortiNAC allows for configuration changes on switches and wireless products from an extended range of vendors. It amplifies the reach of the Security Fabric across multi-cloud, hybrid IT, and heterogeneous environments, implementing “never trust, always verify” principles.

Automated Responsiveness

FortiNAC reacts to network events in real-time to contain threats before they spread, utilizing a broad and customizable set of automation policies. Leveraging AI, these policies can instantly trigger configuration changes and remediation actions when targeted behavior or anomalies are observed, aligning with the Zero Trust model's dynamic and proactive approach.

Next-Gen FortiNAC-F

FortiNAC introduces the Next-Gen FortiNAC-F OS with hardened virtual and physical appliances that increase security and compliance capabilities. Following the tradition of providing the reliable platforms of Fortinet, the new FortiNAC-F will extend the performance capability and introduce new features.

Highlights

Granular Device Visibility

The essence of securing a dynamic, ever-evolving network lies in comprehending its makeup. FortiNAC leverages AI and machine learning from FortiGuard Security Services, goes beyond merely “seeing” everything on the network—it comprehends and analyzes. It scans your network to discover every user, application, and device. Using a variety of techniques—it profiles each element based on observed behavior, real-time threat intelligence, as well as tapping into FortiGuard IoT Services, a cloud-based database for identification lookups.

Scanning can be active or passive, utilizing permanent agents, dissolvable agents, or agentless approaches. Moreover, FortiNAC can evaluate a device against pre-approved profiles, noting any discrepancies or software updates required to patch vulnerabilities. With FortiNAC, the network isn't just known—it's understood, assessed, and continually monitored.

Besides recognizing the entire network, FortiNAC's advanced visibility incorporates passive traffic analysis, leveraging Fortinet FortiGate appliances as sensors to identify anomalous behavior patterns. These patterns can indicate a potential compromise, triggering real-time alerts for the SOC team and aligning with the proactive threat containment approach integral to the Zero Trust model.



FortiNAC 21 Profiling Methods for Device Classification



Highlights



Network Security and Intelligent Segmentation

After successful classification of devices and user identification, FortiNAC now integrates advanced segmentation techniques to ensure only authorized users and devices have access to requisite resources, thus preventing unauthorized intrusion. Through its progressive role-based network access control, FortiNAC allows for strategic network segmentation by logically grouping similar data and applications, limiting access to a particular set of users or devices. This strategy effectively confines a compromised device, thereby inhibiting its ability to traverse the network and inflict damage on other resources. FortiNAC not only fortifies the protection of sensitive data and vital assets but also ensures adherence to internal, industrial, and government regulations and mandates.



Device Integrity Verification and Malware Prevention

FortiNAC emphasizes on the importance of device integrity prior to network connection, significantly reducing the risk and potential spread of malicious software. As a device attempts to join or re-join the network, FortiNAC assesses its configuration for compliance. Any non-compliant configuration is promptly managed; for instance, the device may be allocated to an isolated or restricted access VLAN, devoid of any access to corporate resources. This feature has become increasingly relevant with the rise of IoT devices and remote work trends, ensuring a secure and controlled network environment.



Intelligent Monitoring and Automated Reaction

FortiNAC proactively supervises the network continuously, examining endpoints to verify their compliance with predefined profiles. Leveraging modern security tactics, FortiNAC rescreens devices to prevent any possible bypassing of network access security via MAC-address spoofing. Further, FortiNAC is equipped to identify irregularities in traffic patterns, a vital feature considering the growing complexities in network usage patterns with the rise of cloud and edge computing. This passive anomaly detection function operates symbiotically with FortiGate appliances. Upon recognizing a compromised or susceptible endpoint as a potential risk, FortiNAC promptly instigates an automated reaction, quarantining the endpoint in real-time, furthering its commitment to maintaining a secure and controlled network environment.

Highlights

FortiGate Sessions View

The FortiGate Sessions view adds the ability to accept netflow data from third party devices. Flows from other devices would also show up in this view.

FortiNAC

Dashboard

Users & Hosts

FortiGate Sessions

10.14.14.1@nec.ac

admin

Dashboard

Users & Hosts

FortiGate Sessions

Firewall

Source

Protocol

Source Address

Source MAC Address

Source Port

Destination Address

Destination Port

Added Date

Administrators

Guests & Contractors

Account Requests

Registration Requests

User Accounts

Hosts

Adapters

Applications

Endpoint Fingerprints

Profiled Devices

Device Profiling Rules

FortiGate Sessions

Locate Hosts

Manage Hosts and Ports

Send Message

Network

Policy & Objects

Portal

Logs

System

192.168.1.1

Firewall

udp

10.10.16.11

00:50:56:85:D9:13

56921

8.8.8.8

53

2023/07/28 12:13:12

192.168.1.1

Firewall

tcp

10.10.16.11

00:50:56:85:D9:13

64909

104.117.233.39

443

2023/07/28 12:13:12

192.168.1.1

Firewall

tcp

10.10.16.11

00:50:56:85:D9:13

64911

51.105.71.137

443

2023/07/28 12:13:12

192.168.1.1

Firewall

tcp

10.10.16.11

00:50:56:85:D9:13

64912

20.189.173.4

443

2023/07/28 12:13:12

192.168.1.1

Firewall

tcp

10.10.16.11

00:50:56:85:D9:13

64908

20.125.63.4

443

2023/07/28 12:13:12

192.168.1.1

Firewall

udp

10.10.16.11

00:50:56:85:D9:13

61335

8.8.8.8

53

2023/07/28 12:13:12

192.168.1.1

Firewall

udp

10.10.16.11

00:50:56:85:D9:13

56220

8.8.8.8

53

2023/07/28 12:13:12

192.168.1.1

Firewall

tcp

10.10.16.11

00:50:56:85:D9:13

64914

204.79.197.239

443

2023/07/28 12:21:49

192.168.1.1

Firewall

udp

10.10.16.11

00:50:56:85:D9:13

62066

8.8.8.8

53

2023/07/28 12:21:49

192.168.1.1

Firewall

udp

10.10.16.11

00:50:56:85:D9:13

58963

8.8.8.8

53

2023/07/28 12:21:49

192.168.1.1

Firewall

udp

10.10.16.11

00:50:56:85:D9:13

50252

8.8.8.8

53

2023/07/28 12:21:49

192.168.1.1

Firewall

udp

10.10.16.11

00:50:56:85:D9:13

51513

8.8.8.8

53

2023/07/28 12:23:41

192.168.1.1

Firewall

udp

10.10.16.11

00:50:56:85:D9:13

57210

8.8.4.4

443

2023/07/28 12:23:41

192.168.1.1

Firewall

tcp

10.10.16.11

00:50:56:85:D9:13

64919

142.250.188.3

443

2023/07/28 12:23:41

192.168.1.1

Firewall

tcp

10.10.16.11

00:50:56:85:D9:13

64920

142.251.46.227

443

2023/07/28 12:23:41

192.168.1.1

Firewall

tcp

10.10.16.11

00:50:56:85:D9:13

64928

142.251.46.226

443

2023/07/28 12:23:41

192.168.1.1

Firewall

udp

10.10.16.11

00:50:56:85:D9:13

55942

142.250.189.170

443

2023/07/28 12:23:41

192.168.1.1

Firewall

tcp

10.10.16.11

00:50:56:85:D9:13

64922

142.250.189.238

443

2023/07/28 12:23:41

192.168.1.1

Firewall

udp

10.10.16.11

00:50:56:85:D9:13

51058

142.250.191.74

443

2023/07/28 12:23:41

192.168.1.1

Firewall

udp

10.10.16.11

00:50:56:85:D9:13

59218

142.250.188.14

443

2023/07/28 12:23:41

192.168.1.1

Firewall

udp

10.10.16.11

00:50:56:85:D9:13

63289

142.251.46.195

443

2023/07/28 12:23:41

192.168.1.1

Firewall

udp

10.10.16.11

00:50:56:85:D9:13

62575

8.8.8.8

53

2023/07/28 12:23:41

192.168.1.1

Firewall

tcp

10.10.16.11

00:50:56:85:D9:13

64929

142.250.188.14

443

2023/07/28 12:23:41

192.168.1.1

Firewall

tcp

10.10.16.11

00:50:56:85:D9:13

64917

142.250.189.238

443

2023/07/28 12:23:41

192.168.1.1

Firewall

tcp

10.10.16.11

00:50:56:85:D9:13

64925

142.250.189.170

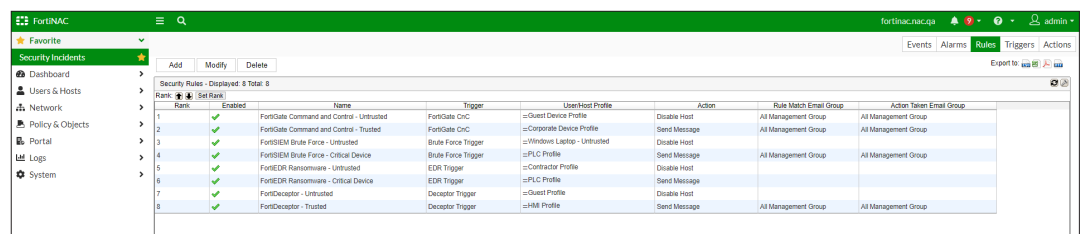
443

2023/07/28 12:23:41

FortiNAC 21 Profiling Methods for Device Classification

Security Fabric Integrations

FortiNAC integrates with multiple Fortinet products such as FortiGate, FortiSIEM, FortiAnalyzer, FortiEDR, FortiDeceptor, FortiClient EMS, FortiLAN Cloud, FortiSwitch, FortiAP, and FortiExtender. The security rules are triggered by syslog/snmp messages from the other Fortinet products as shown below.

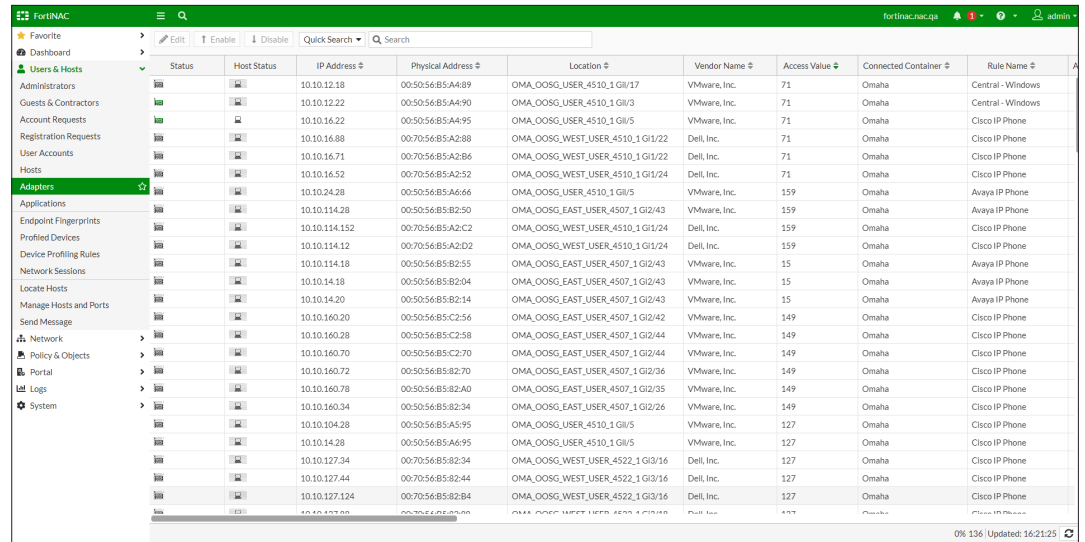


Rank	Enabled	Name	Trigger	User/Host Profile	Action	Rule Match Email Group	Action Taken Email Group
1	✓	FortiGate Command and Control - Untrusted	FortiGate CnC	=Guest Device Profile	Disable Host	All Management Group	All Management Group
2	✓	FortiGate Command and Control - Trusted	FortiGate CnC	=Corporate Device Profile	Send Message	All Management Group	All Management Group
3	✓	FortiSIEM Brute Force - Untrusted	Brute Force Trigger	=Unknown Laptop - Untrusted	Disable Host	All Management Group	All Management Group
4	✓	FortiSIEM Brute Force - Critical Device	Brute Force Trigger	=PLC Profile	Send Message	All Management Group	All Management Group
5	✓	FortiEDR Ransomware - Untrusted	EDR Trigger	=Contractor Profile	Disable Host	All Management Group	All Management Group
6	✓	FortiEDR Ransomware - Critical Device	EDR Trigger	=PLC Profile	Send Message	All Management Group	All Management Group
7	✓	FortiDeceptor - Untrusted	Deceptor Trigger	=Guest Profile	Disable Host	All Management Group	All Management Group
8	✓	FortiDeceptor - Trusted	Deceptor Trigger	=HR Profile	Send Message	All Management Group	All Management Group

FortiNAC Security Rules



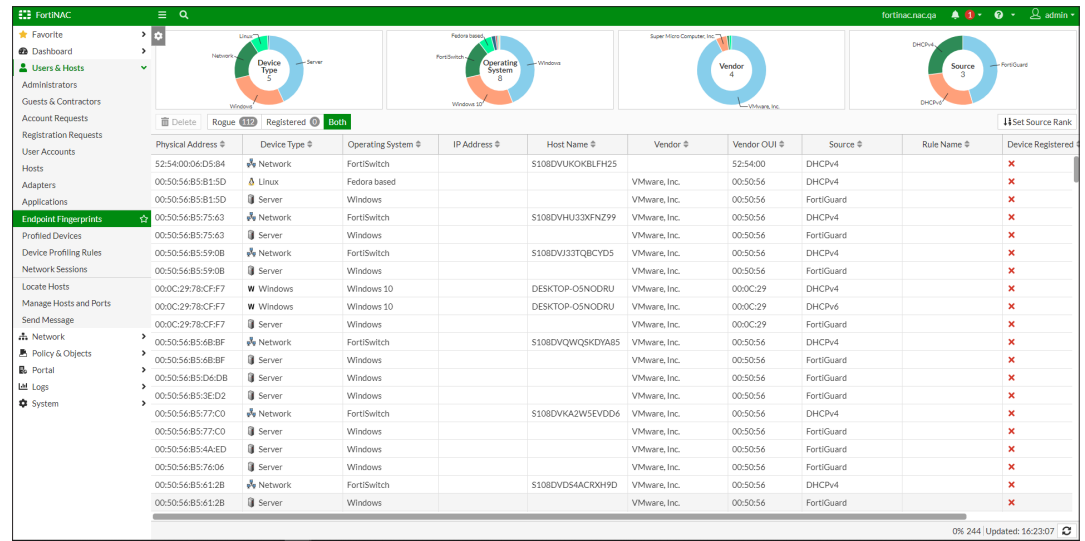
FortiNAC Device and Network View



The screenshot shows the FortiNAC web interface with the 'Device and Network View' selected. The left sidebar contains navigation options like Dashboard, Users & Hosts, Administrators, Guests & Contractors, Account Requests, Registration Requests, User Accounts, Hosts, Adapters, Applications, Endpoint Fingerprints, Profiled Devices, Device Profiling Rules, Network Sessions, Locate Hosts, Manage Hosts and Ports, Send Message, Network, Policy & Objects, Portal, Logs, and System. The main area displays a table of network devices with columns for Status, Host Status, IP Address, Physical Address, Location, Vendor Name, Access Value, Connected Container, and Rule Name. The table lists various devices including VMWare, Inc. and Dell, Inc. with their respective IP and physical addresses, locations, and associated rules.

Status	Host Status	IP Address	Physical Address	Location	Vendor Name	Access Value	Connected Container	Rule Name
		10.10.12.18	00:50:56:B5:A4:89	OMA_OOSQ_USER_4510_1 Gi/17	VMware, Inc.	71	Omaha	Central - Windows
		10.10.12.22	00:50:56:B5:A4:90	OMA_OOSQ_USER_4510_1 Gi/3	VMware, Inc.	71	Omaha	Central - Windows
		10.10.16.22	00:50:56:B5:A4:95	OMA_OOSQ_USER_4510_1 Gi/5	VMware, Inc.	71	Omaha	Cisco IP Phone
		10.10.16.88	00:70:56:B5:A2:88	OMA_OOSQ_WEST_USER_4510_1 Gi/22	Dell, Inc.	71	Omaha	Cisco IP Phone
		10.10.16.71	00:70:56:B5:A2:86	OMA_OOSQ_WEST_USER_4510_1 Gi/22	Dell, Inc.	71	Omaha	Cisco IP Phone
		10.10.16.52	00:70:56:B5:A2:52	OMA_OOSQ_WEST_USER_4510_1 Gi/24	Dell, Inc.	71	Omaha	Cisco IP Phone
		10.10.24.28	00:50:56:B5:A6:66	OMA_OOSQ_USER_4510_1 Gi/5	VMware, Inc.	159	Omaha	Avaya IP Phone
		10.10.114.28	00:50:56:B5:B2:50	OMA_OOSQ_EAST_USER_4507_1 Gi2/43	VMware, Inc.	159	Omaha	Avaya IP Phone
		10.10.114.152	00:70:56:B5:A2:C2	OMA_OOSQ_WEST_USER_4510_1 Gi/24	Dell, Inc.	159	Omaha	Cisco IP Phone
		10.10.114.12	00:70:56:B5:A2:D2	OMA_OOSQ_WEST_USER_4510_1 Gi/24	Dell, Inc.	159	Omaha	Cisco IP Phone
		10.10.114.18	00:50:56:B5:B2:55	OMA_OOSQ_EAST_USER_4507_1 Gi2/43	VMware, Inc.	15	Omaha	Avaya IP Phone
		10.10.14.18	00:50:56:B5:B2:04	OMA_OOSQ_EAST_USER_4507_1 Gi2/43	VMware, Inc.	15	Omaha	Avaya IP Phone
		10.10.14.20	00:50:56:B5:B2:14	OMA_OOSQ_EAST_USER_4507_1 Gi2/43	VMware, Inc.	15	Omaha	Avaya IP Phone
		10.10.160.30	00:50:56:B5:C2:56	OMA_OOSQ_EAST_USER_4507_1 Gi2/42	VMware, Inc.	149	Omaha	Cisco IP Phone
		10.10.160.28	00:50:56:B5:C2:58	OMA_OOSQ_EAST_USER_4507_1 Gi2/44	VMware, Inc.	149	Omaha	Cisco IP Phone
		10.10.160.70	00:50:56:B5:C2:70	OMA_OOSQ_EAST_USER_4507_1 Gi2/44	VMware, Inc.	149	Omaha	Cisco IP Phone
		10.10.160.72	00:50:56:B5:C2:70	OMA_OOSQ_EAST_USER_4507_1 Gi2/36	VMware, Inc.	149	Omaha	Cisco IP Phone
		10.10.160.78	00:50:56:B5:B2:A0	OMA_OOSQ_EAST_USER_4507_1 Gi2/35	VMware, Inc.	149	Omaha	Cisco IP Phone
		10.10.160.34	00:50:56:B5:B2:34	OMA_OOSQ_EAST_USER_4507_1 Gi2/26	VMware, Inc.	149	Omaha	Cisco IP Phone
		10.10.104.28	00:50:56:B5:A5:95	OMA_OOSQ_USER_4510_1 Gi/5	VMware, Inc.	127	Omaha	Cisco IP Phone
		10.10.14.28	00:50:56:B5:A6:95	OMA_OOSQ_USER_4510_1 Gi/5	VMware, Inc.	127	Omaha	Cisco IP Phone
		10.10.127.34	00:70:56:B5:B2:34	OMA_OOSQ_WEST_USER_4522_1 Gi3/16	Dell, Inc.	127	Omaha	Cisco IP Phone
		10.10.127.44	00:70:56:B5:B2:44	OMA_OOSQ_WEST_USER_4522_1 Gi3/16	Dell, Inc.	127	Omaha	Cisco IP Phone
		10.10.127.124	00:70:56:B5:B2:84	OMA_OOSQ_WEST_USER_4522_1 Gi3/16	Dell, Inc.	127	Omaha	Cisco IP Phone

FortiNAC Adapter View



The screenshot shows the FortiNAC web interface with the 'New Endpoint Fingerprints View' selected. The left sidebar is the same as the previous view. The main area displays four donut charts representing different categories: Device Type 5, Operating System 5, Vendor 4, and Source 3. Below the charts is a table of endpoint fingerprints with columns for Physical Address, Device Type, Operating System, IP Address, Host Name, Vendor, Vendor OUI, Source, Rule Name, and Device Registered. The table lists various devices including VMWare, Inc. and FortiGuard, with their respective IP and physical addresses, operating systems, and associated rules.

Physical Address	Device Type	Operating System	IP Address	Host Name	Vendor	Vendor OUI	Source	Rule Name	Device Registered
52:54:00:06:D5:B4	Network	FortiSwitch		S108DVUKOKBLFH25		52:54:00	DHCPv4		X
00:50:56:B5:B1:5D	Linux	Fedora based			VMware, Inc.	00:50:56	DHCPv4		X
00:50:56:B5:B1:5D	Server	Windows			VMware, Inc.	00:50:56	FortiGuard		X
00:50:56:B5:75:63	Network	FortiSwitch		S108DVHU33XFNZ99	VMware, Inc.	00:50:56	DHCPv4		X
00:50:56:B5:75:63	Server	Windows			VMware, Inc.	00:50:56	FortiGuard		X
00:50:56:B5:59:0B	Network	FortiSwitch		S108DVJ37QBQYD5	VMware, Inc.	00:50:56	DHCPv4		X
00:50:56:B5:59:0B	Server	Windows			VMware, Inc.	00:50:56	FortiGuard		X
00:0C:29:78:CF:F7	Windows	Windows 10		DESKTOP-OSNODRU	VMware, Inc.	00:0C:29	DHCPv4		X
00:0C:29:78:CF:F7	Windows	Windows 10		DESKTOP-OSNODRU	VMware, Inc.	00:0C:29	DHCPv6		X
00:0C:29:78:CF:F7	Server	Windows			VMware, Inc.	00:0C:29	FortiGuard		X
00:50:56:B5:6B:BF	Network	FortiSwitch		S108DVQWQKDYA85	VMware, Inc.	00:50:56	DHCPv4		X
00:50:56:B5:6B:BF	Server	Windows			VMware, Inc.	00:50:56	FortiGuard		X
00:50:56:B5:D6:DB	Server	Windows			VMware, Inc.	00:50:56	FortiGuard		X
00:50:56:B5:3E:D2	Server	Windows			VMware, Inc.	00:50:56	FortiGuard		X
00:50:56:B5:77:C0	Network	FortiSwitch		S108DVKA2W5EVD06	VMware, Inc.	00:50:56	DHCPv4		X
00:50:56:B5:77:C0	Server	Windows			VMware, Inc.	00:50:56	FortiGuard		X
00:50:56:B5:4A:ED	Server	Windows			VMware, Inc.	00:50:56	FortiGuard		X
00:50:56:B5:76:06	Server	Windows			VMware, Inc.	00:50:56	FortiGuard		X
00:50:56:B5:61:2B	Network	FortiSwitch		S108DVS4ACRKH9D	VMware, Inc.	00:50:56	DHCPv4		X
00:50:56:B5:61:2B	Server	Windows			VMware, Inc.	00:50:56	FortiGuard		X

FortiNAC New Endpoint Fingerprints View

Third Party Ecosystem Integration

Extensive integration with desktop security software, directories, network infrastructure, and third-party security systems provides unparalleled visibility and control across the network environment.

The FortiNAC family integrates

- More than 3000 devices with unique MIB OIDs
 - More than 2000 models including switches, access points, and network controllers
 - More than 90 vendors in networking, security, and communication industries
- with the following vendor and models as examples*.

Network Infrastructure	Adtran, Aerohive, Alaxala Networks, Alcatel-Lucent, Allied Telesis, Alteon, APC, Apple, APRESIA Systems, Avaya, Brocade/Foundry Networks/Ruckus, Cisco/Meraki, D-Link, Extreme/Enterasys/Siemens, H3C, HP/Colubris/3Com/Aruba, Intel, Juniper, NEC, Riverbed/Xirrus, and SonicWall
Security Infrastructure	CheckPoint, Cisco/SourceFire, Cyphort, FireEye, Juniper/Netscreen, Qualys, Sonicwall, Tenable
Authentication and Directory Services	RADIUS — Cisco ACS, Free RADIUS, Microsoft IAS, Microsoft Entra ID LDAP — Google SSO, Microsoft Active Directory, OpenLDAP
Operating Systems	Android, Apple MAC OSX and iOS, Linux, Microsoft Windows
Endpoint Security Applications	Authentium, Avast, AVG, Avira, Blink, Bullguard, CA, ClamAV, Dr. Web, Enigma, ESET, F-Prot, F-Secure, G Data, Intego, Javacool, Lavasoft, Lightspeed, McAfee, Microsoft, MicroWorld, Norman, Norton, Panda, PC Tools, Rising, Softwin, Sophos, Spyware Bot, Sunbelt, Symantec, Trend Micro, Vexira, Webroot SpySweeper, Zone Alarm
Mobile Device Management	AirWatch, Google GSuite, MaaS360, Microsoft Intune, Mobile Iron, XenMobile, JAMF, Nozomi Networks, Armis, Claroty

* FortiNAC can be integrated with other vendors and technologies in addition to those listed here. This list represents integrations that have been validated in both test lab and production network environments.



Deployment Options

Straight Forward Deployment with Seamless Integration

FortiNAC is a flexible and scalable solution that spans from mid-size to very large enterprise deployments. There are three elements to the FortiNAC solution.

- Application and Control (required)
- Management (optional)
- FortiAnalyzer for Reports (optional)

The Application provides the visibility, and the Control provides the configuration capabilities and automated responsiveness features. The Management portion enables the sharing of concurrent users across a multi-server deployment. FortiAnalyzer provides reports and analytics based on the information gathered from the network through FortiNAC.

FortiNAC can be deployed in on-premise and cloud environments or as hardware appliances, the supported list of hypervisors and Cloud Marketplaces are as:

Hypervisors	Cloud Marketplace
Broadcom VMWare	Microsoft Azure
Microsoft Hyper-V	Amazon AWS
Nutanix	Google GCP
Linux KVM	Oracle OCI
	Alibaba Cloud

The Application and Control Servers can be deployed in a variety of sizes, depending on the number of managed endpoints they need to support. FortiNAC is ideal for supporting distributed architectures including SD-Branch locations.

High Availability

FortiNAC offers High Availability for disaster recovery to ensure redundancy. This state is achieved through active and passive instances where the passive (backup) becomes active when the main is no longer functioning normally. FortiNAC Manager can manage multiple high availability clusters distributed throughout the network as needed.

N+1 Failover Group

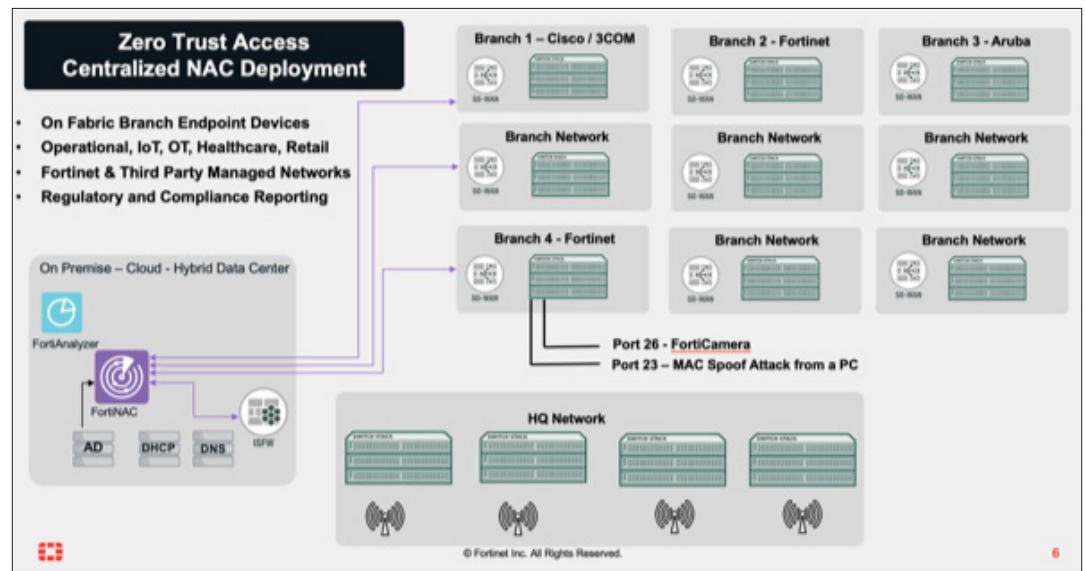
FortiNAC also extend the deployment support to N+1 Failover Group which consist of robust configuration that ensures high availability and redundancy. Can be deployed on shared IP address when all the FortiNAC CAs are in the same subnet for very larger enterprises which are distributed environments. To fully leverage this setup, it's essential to integrate a load balancer to manage traffic distribution and provide automatic failover between the primary and secondary failover group nodes.



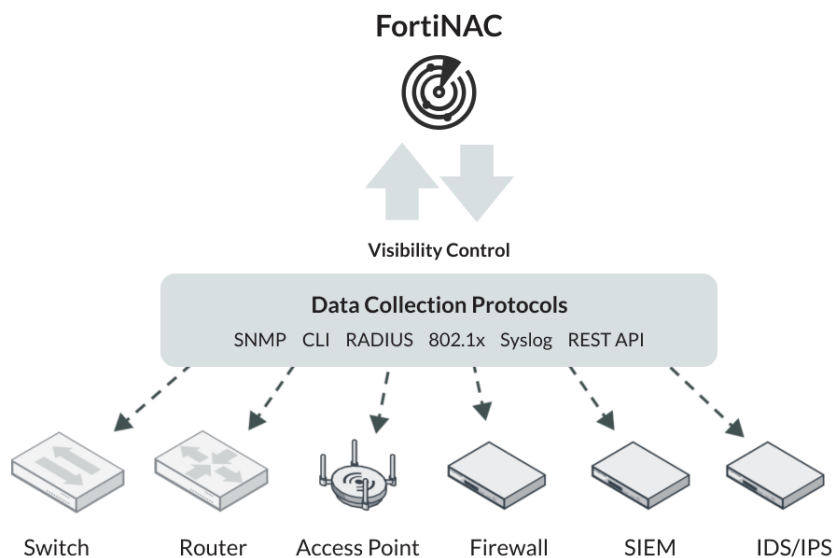
Deployment Options

Centralized Architecture

FortiNAC is an 'out of band' solution, meaning it does not sit in-line of user traffic. This architecture allows FortiNAC to be deployed centrally and manage many remote locations. Visibility, control, and response are achieved by integrating with, and leveraging the capabilities of, the network infrastructure. Control can be applied at the point of connection, at the very edge of the network while security device integrations allow FortiNAC to process security alerts and treat them as triggers for automated threat mitigation through customizable work flows.



Data collection is gathered from multiple sources using a variety of methods. SNMP, CLI, RADIUS, SYSLOG, API and DHCP fingerprints can all be used to achieve the detailed end-to-end visibility necessary to create a truly secure environment.



Licensing

FortiNAC Licensing

FortiNAC offers flexible deployment options based on the level of coverage and functionality desired.

Plus License

The PLUS license level builds on comprehensive features with enhanced visibility and advanced Network Access Controls and automated provisioning for users, guests, and devices as well as reporting and analytics. The reporting and analytics can greatly assist in providing audit documentation of compliance. The PLUS license level is appropriate for organizations that want complete endpoint visibility and a granular control, but do not require automated threat response.

Pro License

The PRO license level provides the ultimate in visibility, control and response. PRO license offers real-time endpoint visibility, comprehensive access control, and automated threat response and delivers contextual information with triaged alerts. The PRO license level is appropriate for organizations that want complete endpoint visibility, a flexible NAC solution with granular controls, as well as accurate event triage and real-time automated threat response.



Licensing

		FORTINAC LICENSE TYPES	PLUS	PRO
Visibility	Network	Network Discovery	✓	✓
		Rogue Identification	✓	✓
		Device Profiling and Classification	✓	✓
	Endpoint	Enhanced Visibility	✓	✓
		Anomaly Detection	✓	✓
		MDM Integration	✓	✓
		Persistent Agent	✓	✓
	User	Authentication	✓	✓
		Captive Portal	✓	✓
	Automation / Control		Network Access Policies	✓
IoT Onboarding with Sponsor			✓	✓
Rogue Device Detection and Restriction			✓	✓
Firewall Segmentation			✓	✓
MAC Address Bypass (MAB)			✓	✓
Full RADIUS (EAP)			✓	✓
BYOD / Onboarding			✓	✓
Guest Management			✓	✓
Endpoint Compliance			✓	✓
Web and Firewall Single Sign-on			✓	✓
Incident Response		Event Correlation		✓
		Extensible Actions and Audit Trail		✓
		Alert Criticality and Routing		✓
		Guided Triage Workflows		✓
Integrations		Inbound Security Events		✓
		Outbound Security Events	✓	✓
		REST API	✓	✓
Reporting		Customizable Reports	✓	✓



Services



FortiCare Services

As your business rapidly evolves, it is critical to advance your security capabilities as well. Often though, you do not have expertise within your organization to deploy, operate, and maintain these new capabilities or are up against tight deadlines to implement change. We understand this challenge and help thousands of organizations every year tackle this problem with FortiCare Services.

Our experts provide accelerated implementation of your technology, reliable assistance through advanced support, and proactive care to ensure your success with Fortinet investment. No matter the size or location of your organization, we are ready to provide you with an elevated experience to help you achieve your business goals with superior security and performance.



FortiCare Support

A FortiCare Support contract entitles you not only to receive updates to the FortiNAC firmware, but also receive two important feeds.

1. Network device database update FortiNAC supports more than 2500 switching, wireless, or firewall devices on the market. As new devices are released, FortiNAC's network device database should be updated to reflect these new models. The weekly update from the FortiNAC team will keep your deployment up to date.
2. FortiGuard IoT Service. One of the means that FortiNAC has to identify devices is to use the cloud-look up service hosted by FortiGuard Labs. A FortiCare Support contract entitles you to use that service at no additional cost, giving you access to a database of millions of devices.

Specifications

	FNC-M-550F	FNC-CA-600F	FNC-CA-500F	FNC-CA-700F
System				
CPU	AMD EPYC 7413 24 Core, 2.65GHz Base Freq.	AMD EPYC 7413 24 Core, 2.65GHz Base Freq.	Intel Xeon E-2278GE 8 Core, 3.3GHz Base Freq.	AMD EPYC 7543P 32 Core, 2.8GHz Base Freq.
Memory	32GB DDR4 memory	32GB DDR4 memory	16GB DDR4 memory	96GB DDR4 memory
Hard Disk	2× 960GB SSDs	2× 960GB SSDs	2× 960GB SSDs	2× 960GB SSDs
BMC	N/A	N/A	N/A	N/A
Network Interface	1x GbE RJ45 and 4× 1GbE SFP or 10GbE SFP+	1x GbE RJ45 and 4× 1GbE SFP or 10GbE SFP+	4x GbE RJ45	1x GbE RJ45 and 4× 1GbE SFP or 10GbE SFP+
RAID Card	N/A	N/A	N/A	N/A
RAID Configuration	Software RAID1	Software RAID1	Software RAID1	Software RAID1
Console Access	RJ45 type COM port for CLI	RJ45 type COM port for CLI	RJ45 type COM port for CLI	RJ45 type COM port for CLI
Form Factor	1U Rack Mount	1U Rack Mount	1U Rack Mount	1U Rack Mount
Dimensions				
Height x Width x Length (inches)	1.73 × 17.20 × 24	1.73 × 17.20 × 24	1.73 × 17.32 × 19.69	1.73 × 17.20 × 24
Height x Width x Length (mm)	44 × 437 × 610	44 × 437 × 610	44 × 440 × 500	44 × 437 × 610
Weight	41 lbs (18.6 kg)	41 lbs (18.6 kg)	32 lbs (14.51 kg)	41 lbs (18.6 kg)
Environment				
Power Supply	Hot Plug, 1+1 Redundant PSU	Hot Plug, 1+1 Redundant PSU	Hot Plug, 1+1 Redundant PSU	Hot Plug, 1+1 Redundant PSU
Input Power	225 watt	225 watt	174 Watt	375 Watt
Input Current	2.3A@100V, 0.94A@240V	2.3A@100V, 0.94A@240V	1.5A@100V; 0.625A@240V	3.75A@100V, 1.57A@240V
Cooling	5x system fans	5x system fans	4x system fans	5x system fans
Panel Display	N/A	N/A	N/A	N/A
Heat Dissipation	767.73 BTU/h	767.73 BTU/h	511.82 BTU/h	1279.553112375 BTU/h
Operation Temperature Range	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)
Storage Temperature Range	-4°F to 158°F (-20°C to 70°C)	-4°F to 158°F (-20°C to 70°C)	-4°F to 158°F (-20°C to 70°C)	-4°F to 158°F (-20°C to 70°C)
Humidity (Operating) Humidity (Non-operating)	5% to 90% non-condensing	5% to 90% non-condensing	5% to 90% non-condensing	5% to 90% non-condensing
Certification				
Safety	Certified as applicable by Product Safety authorities worldwide, including United States (NRTL), Canada (SCC), and European Union (CE).			
Electromagnetic (EMC)	Certified as applicable by EMC authorities worldwide, including United States (FCC), Canada (ICES), and European Union (CE).			
Materials	Certified as applicable by Materials authorities worldwide, including European Union (ROHS) and China (ROHS).			

* The console port can be used for access if the appliance has an issue i.e. you can connect a monitor and a keyboard to it. FortiNAC does not use the console port for access

Visit <https://www.fortinet.com/resources/ordering-guides> for related ordering guides.



Hardware Server Sizing

Appliance



HARDWARE			
Hardware Server	Type	Target Environment	Capacity ¹
FortiNAC-CA-500F	Standalone Appliance (Integrated Control Server and Application Server)	Small Environments	Manages up to 15 000 endpoints
FortiNAC-CA-600F	High Performance Control and Application Server	Medium Environments	Manages up to 30 000 endpoints
FortiNAC-CA-700F	Ultra High Performance Control and Application Server	Large Environments with few Persistent Agents	Manages up to 50 000 endpoints
FortiNAC-M-550F	Management Appliance (Provides centralized management when multiple appliances are deployed)	Multi-site environments with multiple appliances	Can manage up to 100 CA servers with latencies up to 600ms in lab environment

¹ Managed Endpoints = Endpoint devices registered, managed, and enforced by FortiNAC.

VM Server Resource Sizing

Virtual



VIRTUAL MACHINE							
VM OS	SKU	Managed Endpoints ¹	Target Environment	CPU Reference	vCPU Qty ²	Memory (GB)	Disk (GB)
FortiNAC-OS	FNC-CAX-VM	Up to 15 000	Small	Intel Xeon E-2278 GE 3.3 GHz 8C/16T	8	16	100
		Up to 30 000	Medium	AMD Milan EPYC 7413 2.65 GHz 24C/48T	24	32	100
		Up to 50 000	Large	AMD Milan EPYC 7543P 2.8 GHz 32C/64T	32	96	100
	FNC-MX-VM	Up to 100 CA Servers	Large	AMD Milan EPYC 7413 2.65 GHz 24C/48T	24	32	100

¹ Managed Endpoints = total of endpoint devices registered, managed, and enforced.

² The values in the vCPU column were determined by using the CPUs in the CPU reference column and are guidelines only. VM resources may vary based on individual environments.

Performance and Scalability

MANAGED DEVICES, SCALABILITY, GUEST SERVICES, AND PROTOCOLS						
Hardware Server	VM-Small	VM-Medium	VM-Large	FortiNAC-CA-500F	FortiNAC-CA-600F	FortiNAC-CA-700F
Managed Endpoints	15 000	30 000	50 000	15 000	30 000	50 000
Managed FortiGates	800	1500	3000	800	1500	3000
FortiGate w/ FortiSwitch (FortiLink)	600	800	1000	600	800	1000
Guest Web Login (Auth / Sec)	30	60	80	100	100	100
Guest Self Registration (Request / Sec)	20	20	20	20	20	20
Netflow (Request / Sec)	400	400	400	400	400	400
Syslog (Request / Sec)	90	90	90	90	90	90
REST API (Request / Sec)	400	400	400	1000	1000	1000

RADIUS PERFORMANCE (REQUEST / SECOND)					
Auth. Outer Method	Auth. Inner Method	Auth Source	FortiNAC-CA-500F	FortiNAC-CA-600F	FortiNAC-CA-700F
PAP	N/A	Local Database	300	600	1000
PAP	N/A	Active Directory	500	900	1000
PEAP	EAP-GTC	Local Database	200	900	1000
PEAP	EAP-GTC	Active Directory	500	1000	1500
PEAP	EAP-MSCHAPv2	Local Database	800	1200	1500
PEAP	EAP-MSCHAPv2	Active Directory	900	1200	1500
EAP-TTLS	EAP-GTC	Local Database	230	400	1000
EAP-TTLS	EAP-GTC	Active Directory	800	1200	1500
EAP-TTLS	EAP-MSCHAPv2	Local Database	800	1000	1500
EAP-TTLS	EAP-MSCHAPv2	Active Directory	800	1200	1500
EAP-TLS	N/A	Local Database	800	1200	1500
EAP-TLS	N/A	Active Directory	800	1200	1500
MAB	N/A	Local Database	900	1200	1500

FORTINAC MANAGER		
	FortiNAC-M-550F	FortiNAC-MX-VM
Max Manager Cluster Nodes	5	5
Max CA Capacity per Node	100	100

In the context of max CA capacity for FortiNAC manager, the system counts only active CAs.

Therefore High-Availability 1+1 counts as 1, and an N+1 failover group counts as N, because the standby node only receives health checks.



Ordering Information

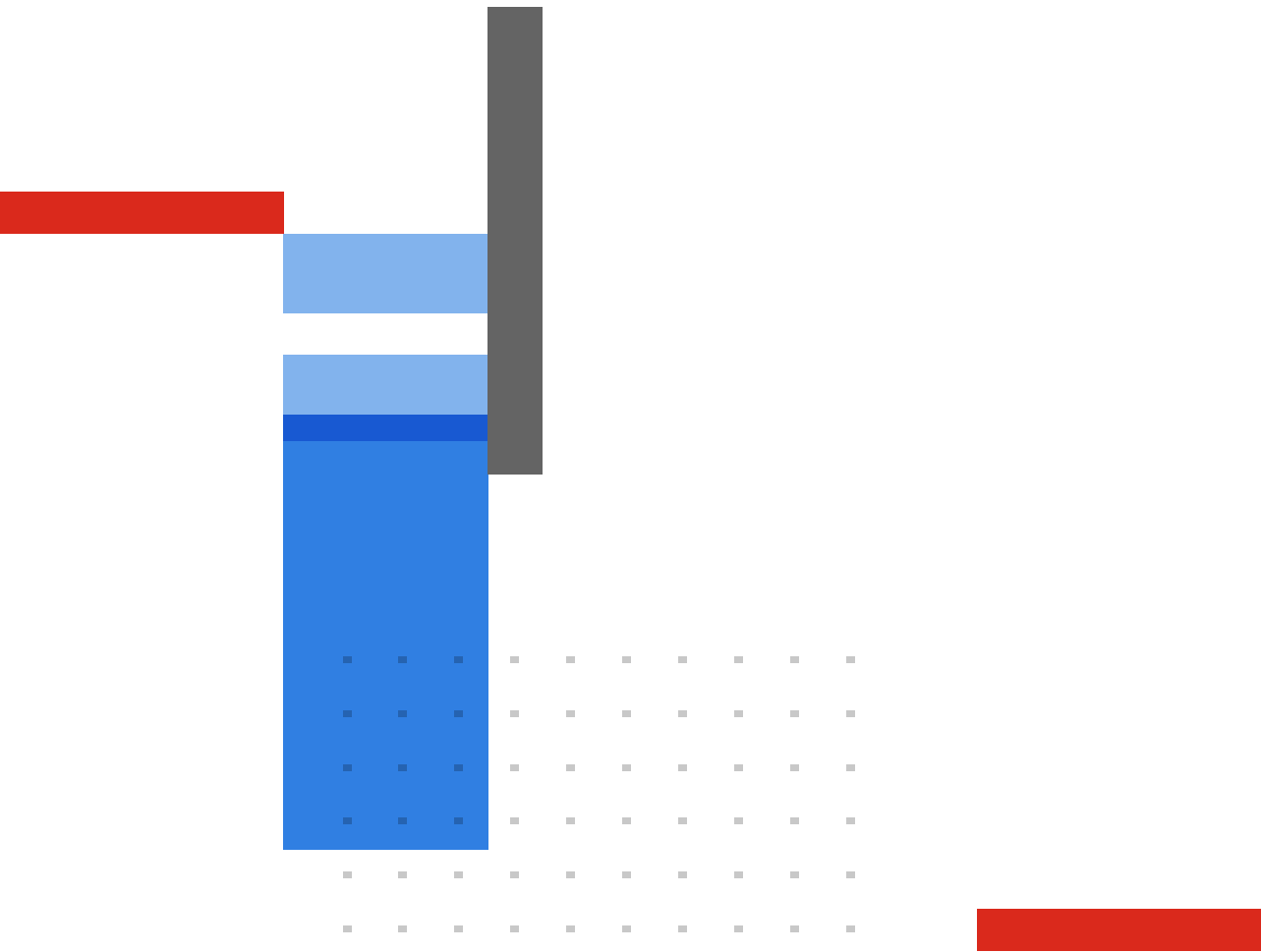
PRODUCT	SKU	DESCRIPTION
Appliances		
FortiNAC-CA-500F	FNC-CA-500F	F series of the FortiNAC CA hardware supporting up to 15 000 endpoints.
FortiNAC-CA-600F	FNC-CA-600F	F series of the FortiNAC CA hardware supporting up to 30 000 endpoints.
FortiNAC-CA-700F	FNC-CA-700F	F series of the FortiNAC CA hardware supporting up to 50 000 endpoints.
FortiNAC-M-550F	FNC-M-550F	F series of the FortiNAC Manager hardware. Supports up to 100 CAs servers.
Virtual Machines		
FortiNAC Control and Application extended VM	FNC-CAX-VM	FortiNAC Control and Application next-gen VM Server supports up to 50 000 endpoint devices. Supporting VMware ESXi / ESX, Microsoft Hyper-V, Linux Kernel-based Virtual Machine (KVM), Nutanix and Cloud providers Amazon AWS, Microsoft Azure, Google GCP, Oracle OCI, and Alibaba Cloud.
FortiNAC Manager extended VM	FNC-MX-VM	FortiNAC Manager next-gen VM Server supports up to 100 CA Servers. Supporting VMware ESXi / ESX, Microsoft Hyper-V, Linux Kernel-based Virtual Machine (KVM), Nutanix and Cloud providers Amazon AWS, Microsoft Azure, Google GCP, Oracle OCI, and Alibaba Cloud.
Perpetual Licenses		
FortiNAC PLUS License 100	LIC-FNAC-PLUS-100	FortiNAC Perpetual PLUS License for 100 concurrent endpoint devices. Provides Endpoint visibility and Dynamic VLAN Steering, Advanced Network Access Controls and automated provisioning for users, guests, and devices.
FortiNAC PLUS License 1K	LIC-FNAC-PLUS-1K	FortiNAC Perpetual PLUS License for 1000 concurrent endpoint devices. Provides Endpoint visibility and Dynamic VLAN Steering, Advanced Network Access Controls and automated provisioning for users, guests, and devices.
FortiNAC PLUS License 10K	LIC-FNAC-PLUS-10K	FortiNAC Perpetual PLUS License for 10 000 concurrent endpoint devices. Provides Endpoint visibility and Dynamic VLAN Steering, Advanced Network Access Controls and automated provisioning for users, guests, and devices.
FortiNAC PLUS License 50K	LIC-FNAC-PLUS-50K	FortiNAC Perpetual PLUS License for 50 000 concurrent endpoint devices. Provides Endpoint visibility and Dynamic VLAN Steering, Advanced Network Access Controls and automated provisioning for users, guests, and devices.
FortiNAC PRO License 100	LIC-FNAC-PRO-100	FortiNAC Perpetual PRO License for 100 concurrent endpoint devices. Pro license level provides the ultimate in visibility, control and response.
FortiNAC PRO License 1K	LIC-FNAC-PRO-1K	FortiNAC Perpetual PRO License for 1000 concurrent endpoint devices. Pro license level provides the ultimate in visibility, control and response.
FortiNAC PRO License 10K	LIC-FNAC-PRO-10K	FortiNAC Perpetual PRO License for 10 000 concurrent endpoint devices. Pro license level provides the ultimate in visibility, control and response.
FortiNAC PRO License 50K	LIC-FNAC-PRO-50K	FortiNAC Perpetual PRO License for 50 000 concurrent endpoint devices. Pro license level provides the ultimate in visibility, control and response.
Subscription Licenses		
FortiNAC Subscription PLUS License	FC5-10-FNAC1-213-01-DD	FortiNAC Subscription PLUS License for 100 concurrent endpoint devices. Provides Endpoint visibility and Dynamic VLAN Steering, Advanced Network Access Controls and automated provisioning for users, guests, and devices. MOQ 100.
	FC6-10-FNAC1-213-01-DD	FortiNAC Subscription PLUS License for 1000 concurrent endpoint devices. Provides Endpoint visibility and Dynamic VLAN Steering, Advanced Network Access Controls and automated provisioning for users, guests, and devices.
	FC7-10-FNAC1-213-01-DD	FortiNAC Subscription PLUS License for 10 000 concurrent endpoint devices. Provides Endpoint visibility and Dynamic VLAN Steering, Advanced Network Access Controls and automated provisioning for users, guests, and devices.
	FC8-10-FNAC1-213-01-DD	FortiNAC Subscription PLUS License for 50 000 concurrent endpoint devices. Provides Endpoint visibility and Dynamic VLAN Steering, Advanced Network Access Controls and automated provisioning for users, guests, and devices.
FortiNAC Subscription PRO License	FC5-10-FNAC1-209-01-DD	FortiNAC Subscription PRO License for 100 concurrent endpoint devices. Pro license level provides the ultimate in visibility, control, and response. MOQ 100.
	FC6-10-FNAC1-209-01-DD	FortiNAC Subscription PRO License for 1000 concurrent endpoint devices. Pro license level provides the ultimate in visibility, control, and response.
	FC7-10-FNAC1-209-01-DD	FortiNAC Subscription PRO License for 10 000 concurrent endpoint devices. Pro license level provides the ultimate in visibility, control, and response.
	FC8-10-FNAC1-209-01-DD	FortiNAC Subscription PRO License for 50 000 concurrent endpoint devices. Pro license level provides the ultimate in visibility, control, and response.

Visit <https://www.fortinet.com/resources/ordering-guides> for related ordering guides.



Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet’s products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the [Fortinet EULA](#) and report any suspected violations of the EULA via the procedures outlined in the [Fortinet Whistleblower Policy](#).



www.fortinet.com

Copyright © 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

A decorative pattern of concentric hexagons in a light blue color, scattered across the top dark blue background.

FortiNAC - Administration Guide

Version F 7.6.5

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com

November 17, 2025

FortiNAC F 7.6.5 Administration Guide

49-20-748677-20210922

TABLE OF CONTENTS

What's new	14
What's New in FortiNAC F 7.6.0	14
First time users	17
FortiNAC	18
Introduction	18
Performance Sizing and Capacity	19
Figures	19
Monitoring	19
Monitor devices	20
View and register known devices	20
Import devices	20
Discovery	21
Register non-SNMP devices	21
Register PCs	21
View devices	21
Learning about hosts on the network	22
Link up and link down traps	22
MAC notification traps	23
Polling	23
Isolate unknown devices	24
VLANs	24
Forced registration group	24
Control access based on device types	24
Disable devices with scheduled tasks	24
Modify device settings	25
Role based access	25
View logs and reports	25
Netflow Support	25
DNS configuration	26
Windows	26
Linux	27
macOS	27
IPv6 support	28
Guided Install	28
Login procedure	28
Connection errors	29
Licenses	29
License count	30
Events and alarms	31
FortiNAC Manager	32
Evaluation license keys	33
Navigation tips	33
Filters	34

Dashboard search	35
Quick search	36
Custom filter	36
CLI Console	40
Wild cards	41
Find containers or devices	41
Download logs	41
Passwords	42
CLI/SSH passwords	42
Administrator passwords	43
Time stamps and time zones	43
Database	43
Display and export	43
Icons	44
Certificates	47
Supported TLS Versions	50
Open ports	50
Related Documents	50
Validate Open Ports	51
FortiNAC Open Port List	51
FortiNAC Access Configuration	51
FortiNAC CA Firewall Policy Requirements	54
FortiNAC Manager Firewall Policy Requirements	57
Fortinet Device Integration Firewall Policy Requirements	59
Third Party Device Integration Firewall Policy Requirements	63
SNMP trap support	67
SSH Algorithm Support	70
Wireless security	71
Auto-configured data	73
SSID mappings	76
Secure SSID for guest management	78
Open SSID for guest management	79
Secure SSID for device onboarding	80
Open SSID for device onboarding	82
Dashboard	86
Terminology	86
Overview	86
Adding widgets	87
Widget Organization	87
Alarms	88
Endpoint Fingerprints	88
Host Summary	89
User Summary	91
License Information	92

Logical network host access	92
Monitors	93
Network Device Summary	93
Pending Tasks	93
Recent hosts	94
System Performance	94
Persistent Agent Summary	95
RADIUS Activity	95
Security Summary	96
Scans	96
System Summary	96
Top host activity	97
Menus	97
Feature Visibility	100
Import and export data	101
Import archived data	102
Import hosts, users or devices	102
Create an import file	102
Sample import files	108
Import from a .csv file	109
Import from a previous version	109
Import an administrator	109
Create an import file	110
Sample import file	111
Import IP ranges	112
CLI import tool	112
Create .csv files for device import	113
Import devices with the CLI tool	115
Import port descriptions	116
Export data	116
Users & Hosts	118
Administrators	119
Add an administrator	121
Modify an administrator	123
Delete an administrator	124
Copy an administrator	124
Modify an administrator profile	124
Administrator profiles	125
Default administrator profiles	126
Permissions list	133
Add an administrator profile	139
Modify administrator profiles	143
Delete an administrator profile	144
Copy an administrator profile	144
Administrator profile mappings	144
Limit access with groups	148

Set privileges based on directory groups	149
Add administrators to groups	150
Group membership	151
Configure secure mode	151
Guests & Contractors	151
Implementation	152
Guest & Contractor users	153
Accounts with sponsor privileges	163
Log in as a sponsor	163
Guest & Contractor templates	164
Administrator profile	174
Add a guest manager profile	175
Add a guest kiosk profile	177
Add a guest self registration profile	178
Administrators	180
Add an administrator	180
Portal page setup	182
Printer settings for guest badges	184
Events and alarms	184
Guest/contractor login	185
Using a kiosk	185
Guest self registration	188
Account requests	191
Registration requests	192
User accounts	194
Navigation, menus, options, and buttons	196
Configure table columns and tooltips	197
Search settings	199
User properties	200
Add or modify a user	202
Delete a user	204
Add users to groups	205
Group membership	205
Guest accounts	206
Add a guest account	206
Portal page requirements	206
Guest account details	207
Set user expiration date	208
Maximum concurrent sessions	210
Vulnerabilities	210
Hosts, adapters, and applications	211
USB/Thunderbolt external Ethernet adapters	211
Thunderbolt adapters and docking stations	211
Host record management when external adapters are moved between hosts	211
Adapter is moved between registered hosts	212
Adapter is moved from a registered host to a rogue	213
Hosts	213
Adapter View	237

Aging out host or user records	241
Application view	243
Endpoint Fingerprints	245
Right-Click Options	247
Profiled devices	251
How it works	251
Configure profiled devices	252
Implementation	255
Profiles for device managers	256
Add an administrator	257
Events and alarms	259
Device profiling rules	259
Network sessions	274
Using filters	274
Creating a device profiling rule	274
Deleting a session	274
Locate hosts	276
Locate devices or hosts	276
Locate hosts and users	276
Edit hosts	279
Locate devices	280
Edit devices	281
Manage hosts and ports	283
Add hosts	283
View hosts and ports	285
View and manage ports	285
Send message	286
Implementation	286
Send messages to hosts	288
Network	289
Inventory	289
Inventory tree contact status	292
Network summary	292
Customer icon	293
Containers	296
Container icon	297
Discovery	311
Discovery results	313
Device view	314
Device properties	323
Device configuration	336
Credentials	351
Ports view	354
SSID view	365
Virtualized Devices	371
Logical networks	373
RADIUS	375
802.1x environments	375

Order of precedence	376
Configuration	376
Legacy Proxy	381
Virtual Servers	392
Configure Local Server	393
Configure Proxy Server	397
Domain Mappings	399
Attribute Groups	400
Winbind	403
Activity	405
Service Connectors	405
Authentication sources	406
Email/SMS	410
MDM Servers	413
OT	416
Security Fabric Connection	420
ServiceNow ITSM Integration	420
FortiEdge Cloud	423
Arista Cloud	425
Check Point Cloud	426
Meraki Cloud	427
Mist Cloud	427
Admin SAML SSO	427
User SAML SSO	427
Vulnerability Scanners	427
Admin FortiCloud SSO	432
CLI configuration	433
Configuration in use	435
Show configuration	435
Port based and host based configurations	435
Add or modify a configuration	436
Implement configurations	439
Requirements for ACL based configurations	446
L2 polling	449
Set L2 polling	450
L3 polling	451
Set L3 polling	452
L3 Device Identification	453
Network events	453
Port changes	455
Policy & Objects	457
Policy overview	458
Policy assignment	458
Policy details	461
Policy simulator	464
User/host profiles	466
Add or modify a profile	468
Filter example	468

Profile example	469
Profiles in use	470
Delete a profile	471
Portal policy	471
Implementation	472
Manage policies	472
Create or edit a policy	473
Delete a policy	475
Authentication	475
Manage policies	476
Create or edit a policy	478
Delete a policy	478
When no profile or policy exists	479
Authentication configurations	479
Add or modify a policy	481
Delete a configuration	481
Network access	482
Implementation	483
Manage policies	484
Create or edit a policy	485
Delete a policy	485
Network access configurations	486
Create or edit a configuration	487
Configurations in use	487
Delete a configuration	487
Endpoint compliance	488
Implementation	489
Agent overview	492
Dissolvable Agent	493
Persistent Agent	495
Mobile Agent	506
Agent server communications	507
SSL certificates	509
Auto-definition updates	531
Policies	531
Add or modify a policy	534
Determining host operating system	534
Create or edit a policy	536
Delete a policy	536
Configurations	536
Create or edit a configuration	537
Configurations in use	540
Delete a configuration	540
Chaining configuration scans	540
Scans	542
Custom scans	560
Windows Custom Scan	570

Registry version scan	577
Registry date scan	578
Scan parameters	581
Actions	591
Supplicant EasyConnect	595
Host configuration process	596
Requirements	596
Manage policies	598
Create or edit a policy	599
Delete a policy	599
Supplicant configurations	600
Create or edit a configuration	601
Configurations in use	603
Delete a configuration	603
Passive Agent	604
Registration	604
Manage configurations	604
Add or modify configuration	606
Delete configuration	607
Copy configuration	607
IP ranges	607
Test a directory user	608
Administrative templates for GPO	608
CLI arguments	615
Remediation configurations	615
Add a scan	616
View scan status	617
Clear scanned hosts list	618
Modify or remove a scan	619
Roles	620
Configuration	621
Assigning roles	621
Roles view	625
Network device roles	627
Portal	631
Portal configuration	631
Content editor	632
Social Media for Captive Portal	661
Version 1 settings	734
Configure authentication credentials	737
Example - change portal image	738
Request Processing Rules	741
Portal SSL	745
Logs	746
Audit Logs	746
Configuration	747
Accessing the auditing log	747

Events	749
Event notes	749
Events and alarms list	750
Event management	772
Enable and disable events	773
Event thresholds	774
Log events to an external log host	776
SNMP trap format	779
Common event format (CEF)	780
Examples of syslog messages	781
View events currently mapped to alarms	782
Alarms	783
Show or hide alarm details	784
Map events to alarms	784
Add or modify alarm mapping	787
Bulk modify alarm mappings	791
Delete alarm mapping	792
Reports	793
Standard report templates	793
Custom reports	798
Schedule reports	802
Archived reports	803
Scan results	804
Show details	804
Archive and clear all scans	805
Archive and clear selected scans	805
Security Incidents	806
Implementation	807
Vendor severity levels	811
Events	814
Alarms	815
Rules	817
Triggers	820
Actions	823
System	827
Certificate management	828
Server certificates	828
High Availability(HA) Certificate Management	830
Trusted certificates	835
Config wizard	839
Cluster Management	839
Modify Nodes	841
Switch Worker to Leader	842
Rebalancing	842
Endpoint Synchronization	842
Groups	843
Add groups	845
Copy a group	845

Delete a group	845
Limit user access with groups	846
Modify a group	846
Group membership	847
Set Host Registration Limit	847
Show group members	851
Group in use	851
Aging hosts in a group	851
System groups	851
Customer defined groups	854
Feature Visibility	856
Scheduler	857
Add a task	858
Add other scheduled tasks	861
Copy a task	861
Delete a task	861
Modify a task	862
Run task now	862
Tasks	862
Settings	863
Authentication	867
Automatic authentication	867
Directories	868
Identification	883
Device types	883
NAT detection	888
Docking Station Management	891
Rogue DHCP server detection	892
Vendor OUIs	898
Roaming guests	901
RADIUS configuration	901
Model configuration	901
Local domains	902
Notes	902
Connection process	902
Add local domains	902
Multi-factor Authentication	903
Overview	903
Types of Multi-Factor Authentication	903
REST SMS Gateway Configuration	903
Control	905
Access point management	905
Allowed domains	907
Network device	910
Persistent Agent	913
Reports	932
Analytics	932
System communication	933

System management	975
Custom Health Check	976
Overview	976
Updates	991
Agent updates	1001
System	1004
Latest/All Upgrades	1004
File Upload	1004
User/Host Management	1006
Aging	1006
Allowed hosts	1008
Device profiler	1008
MAC address exclusion	1009
Change log	1011

What's new

This section covers What's New for FortiNAC version F 7.6.

What's New in FortiNAC F 7.6.0

CentOS Support No Longer Available

Version F 7.6 and greater does not support FortiNAC appliances running the CentOS operating system. Customers with CentOS FortiNAC appliances must migrate to the new FortiNAC-F servers to upgrade to version F 7.6 or greater. Contact sales to obtain the new FortiNAC-F appliances (FNC-CAX-xx/FNC-MX-xx/FortiNAC-CA-xxF). For additional information regarding the migration process, refer to the following documentation under the Admin Guide section of the [Document Library](#):

CentOS to FortiNAC-OS VM Migration: CA Servers

CentOS to FortiNAC-OS VM Migration: Separate C + A Servers

CentOS to FortiNAC-OS Hardware Migration: CA Servers

Access Point Management No Longer Available

The Access Point Manager functionality has been removed as of FortiNAC version F 7.6. Customers using this feature must move to an alternative solution prior to upgrade. For details, see KB article [Access Point Management Removed in Version F 7.6](#)

Check Point VPN Integration

Enable enforcement of endpoint posture for users and machines connected through Check Point VPN. This includes both SSL and remote access VPNs. The feature will ensure that both user login and machine compliance are validated, similar to existing support for Cisco ASA, FortiGate and Palo Alto Networks.

See the following reference manuals:

[Check Point VPN Integration - Central mode \(977261\)](#)

[Check Point VPN integration - Local Mode \(936094\)](#)

Machine authentication

FortiNAC supports Machine Authentication with RBAC based on compute groups in the Active Directory (AD). (1026125)

If the client (host) is in one group inside LDAP, after the group is synced to FortiNAC, the group will be renamed as group_host. If the user selects "group_host" for group attribute, the host will be added to that group_host automatically.

Group feature does not support primary groups such as LDAP Domain Computers group. Please use LDAP groups as alternative.

See the [Machine Authentication](#) cookbook.

Limit maximum number of concurrent sessions

FortiNAC able to limit the maximum number of user concurrent sessions. (1013495)

See [Maximum concurrent sessions](#) in the administration guide.

RADIUS Enhancements

TEAP support for RADIUS Clients (1021352)

TLS 1.3 supported in Local RADIUS Local Servers configuration. (1029125)

See [Configure local server](#) in the administration guide.

Palo Alto Integration enhancements

Support to send Single Sign On (SSO) Tags to Palo Alto Network devices for non-VPN environments. (1026144) (1016612).

See the [Palo Alto Networks Integration](#) guide.

Mist Wireless Integration Enhancements - Added Device Management API Support

FortiNAC is now able to manage the Mist Cloud using Device Management APIs. This is done by using the new Mist Service Connector in the FortiNAC UI. Previously, Mist was modeled in FortiNAC by running the CloudAPITool command in the CLI. See [Mist Wireless Integration Guide](#) for details.

Note: Legacy Mist Wireless integrations that used the CloudAPITool are not automatically migrated to the new Service Connector integration. Transitioning is a manual process that can be done one Mist Site at a time. Remove any existing Access Points from FNAC for the desired site, then use the new Service Connector to select the site. The Access Points for the site are created as pingable devices upon Service Connector Poll.

FortiNAC-F Core Enhancements (FortiNAC Manager and CA)

Cluster Custom health check (1026141)

Assess the health of a CA using certain health check types (i.e. protocols) like ICMP, TCP, and TCP Echo.

See [Custom Health Check](#) in the FortiNAC Manager Guide.

Cluster Management

FortiNAC Manager Cluster Management provides users a central access service to view or modify information from multiple CA's. FortiNAC Managers work together to manage the same CA's so that information is processed timely and effectively for larger environments.



Important: Upgrading to 7.6.0 replaces High Availability (HA) configurations with Cluster Management. This affects FortiNAC Manager HA pairs only. Customers should review the 7.6.0 Release Notes prior to upgrade.

See [Cluster Management](#) in the FortiNAC Manager Guide.

FortiNAC CA (Control & Application) Management

See [CA Management](#) in the FortiNAC Manager Guide.

N+1 Failover

FortiNAC-M functions as a manager to manage the N+1 Failover Groups (defined as one secondary server for one or more primary servers), enabling N+M high availability for CAs.

See the [N+1 Failover Reference Guide](#).

Note: CAs configured for High Availability are still supported.

New Internal DHCP Server

KEA DHCP (1026154)

FortiNAC now uses KEA DHCP as internal server for dynamically assigning addresses to isolated hosts.

See the [Cookbook](#) for the PXE boot use case.

GUI enhancements

Service Connectors GUI Enhancement (1024138)

- Created OT categories for Nozomi and Claroty
- See the updated [MDM/OT guide](#).

7.6 UI/UX Rewrite of the Actions Views (1035739)

FortiNAC New Portal Configuration (1016389)

- New Portal Configuration UI design with a modernized look, unified with FortiGuest.

High Availability: Secondary Server UI now available in standby

- SSL certificate installation (0877961) - See [Certificate Management](#)
- Config Wizard settings - See [Config Wizard](#)

First time users

First time users of the FortiNAC device should follow the steps in the [Deployment Guide](#).

FortiNAC

FortiNAC integrates with your existing desktop security software, network directories and infrastructure, and security solutions. This gives your organization unlimited visibility to which users are on the network, which endpoint devices are on the network, and where and when users and devices are connecting. Additionally, network access policies ensure that confidential resources are secure by tracking which users are allowed to have access, detailing which users may have already accessed those resources, and ensuring that private information remains private. FortiNAC simplifies IT operations by empowering administrators to create security policies that automate control over network access. Finally, our built-in tools and schema enable administrators to build reports for regulatory compliance.

FortiNAC is a flexible, modular security platform that allows solutions to be customized to fit your organization's needs. FortiNAC uses a unique out-of-band architecture that leverages your existing IT infrastructure to provide unparalleled visibility and to enable security policies to be applied automatically across the entire network.

The FortiNAC package installed on your appliance is referred to as FortiNAC throughout the documentation.

If you do not see a feature described in the documentation, it could be for one of the following reasons:

- You may not have purchased all of the features outlined in this documentation.
- You may not have permission to access the feature.

Introduction

This document provides comprehensive information on all of the features available in FortiNAC that are used to enforce network usage policies, monitor specific events, and automatically take actions. When FortiNAC recognizes an event, it takes the defined action, and logs both for tracking purposes.

Configurations using the Administration User Interface of individual FortiNAC components, such as groups and scheduled actions, are included. Components and configurations viewed/modified through the Administration UI and the last known state of those components are stored in the FortiNAC's mysql database. Passwords are encrypted.

Device integration information is provided on the [Fortinet Documentation Library](#).

The [Requirements](#) section defines the host requirements for the FortiNAC administrator. Refer to [Dashboard on page 86](#) topics to get started.

This documentation applies to the FortiNAC Server, FortiNAC Control Server, and FortiNAC Application Server appliances.



Internet Access

It is recommended that FortiNAC has internet access to receive product updates. Internet access allows FortiNAC to stay up to date and secure.

Performance Sizing and Capacity

Figures

The following tables in the [FortiNAC Data Sheet](#) are guidelines to determine the most appropriate FortiNAC server for a customer's environment:

- Hardware Server Sizing
- VM Server Resource Sizing

The criteria used is the total number of ports in the network. If an environment grows beyond the max number of ports specified for a particular server, performance issues can occur due to CPU and memory allocation. In such cases, the FortiNAC system resources should be re-evaluated.

Administrators can utilize tools within the FortiNAC UI to monitor performance. See [Monitoring](#) for more details.

Certain performance-related parameters are modifiable. See [Tuning](#) for more details.

Monitoring

Administrators can monitor the FortiNAC system resources using tools specified in the table below.

See [Events & Alarms](#) List for additional details on each event.

Customers can configure alarms to notify when resources are reaching specific thresholds. See [Event thresholds](#) and [Map events to alarms](#) for details.

	Dashboard Widget	Event/Alarm
CPU Usage	System Performance (Expand widget to view graph)	
Memory Usage	System Performance (Expand widget to view graph)	Memory Usage Process Memory Usage
Disk Utilization	System Performance	Hard Disk Usage
Process Threads	System Performance	Process Thread Count
L2 Polling	Alarms	L2 Poll Failed
L3 Polling	Alarms	L3 Poll Failed

	Dashboard Widget	Event/Alarm
RADIUS	RADIUS	RADIUS Rate
SSO	Alarms	Communication Lost with RADIUS/SSO Agent
License Usage	License Information Tracks Concurrent License counts: In use Available Percentage used	Maximum Concurrent Connections

Monitor devices

FortiNAC provides a window into your network. It allows you to register known devices, isolate unknown devices and see where devices are connected to the network. Devices can be managed or controlled based on device roles.

There are a variety of ways to implement monitoring depending on how you choose to control your network. The implementation process outlined below touches on features within FortiNAC that can be used to control devices. These features are distributed throughout the product, therefore links to relevant sections of the documentation have been provided.

View and register known devices

Provisioning FortiNAC with known devices can be accomplished in several ways. However, you should start with switches, routers and controllers, since those devices control the network and provide FortiNAC with information about other devices connected to the network. Switches, routers and controllers can be imported into FortiNAC from .csv files or can be automatically discovered by FortiNAC. Other devices can be imported or detected as they connect to the network.

Import devices

If you already have spreadsheets or .csv files containing device information, you may be able to leverage them to import devices into FortiNAC. Each device type must be in a separate file. Both SNMP devices and non-SNMP (or pingable) devices can be imported. See [CLI import tool on page 112](#).

Discovery

Discovery is an automated process started by the FortiNAC administrator. FortiNAC searches ranges of IP addresses for devices that can be managed using SNMP. A model of each device is created in FortiNAC as it is discovered and can be viewed in the **Network Devices** view. After discovery, each device must be configured to ensure that FortiNAC has the correct CLI passwords and VLAN configurations.

See [Network devices on page 1](#), [Model configuration on page 338](#), [Network access/VLANs on page 319](#), and [Device properties on page 323](#) for additional information.

Register non-SNMP devices

Most networks also have a series of devices that cannot be managed using SNMP, such as printers, security cameras or alarm systems. This type of device is referred to as a pingable device. Non-SNMP devices can be imported into the database as noted above, can be registered manually or can be automatically registered by device profiler.

For manual registration, you must connect the device to the network. When FortiNAC detects that a device has connected, that device is displayed as a rogue in the Host View. From the Host View you can select one or more rogues and register them as devices. Devices registered from the Host View can be configured to display in the Host View, the Inventory or both. See [Register a host as a device on page 232](#) and [Learning about hosts on the network on page 22](#).

If you have implemented device profiler, devices can be categorized and automatically registered based on Profiling Rules. See [Profiled devices on page 251](#).

Register PCs

Registering PC's as devices can be done manually by connecting the PC to the network. When FortiNAC detects the connection, the PC is displayed in the Host View as a rogue. From the Host View, you can select one or more rogues and register them as devices as noted above. See [Register a host as a device on page 232](#) and [Learning about hosts on the network on page 22](#).

Registering PCs can be automated to a certain extent. You can configure the Persistent Agent to register PCs by hostname using . Then serve the Persistent Agent to users PCs either at login or by asking the user to download and install the agent. The agent connects to the FortiNAC server, registers the PC by hostname and sends information such as IP address and MAC address back to the database. Because the agent is only being used as a mechanism to register PCs, no security policy is required. See [Agent overview on page 492](#) and [Credential configuration on page 918](#).

Login scripts can be used to automatically register PCs as network users log onto the network. The script must be modified slightly to indicate that PCs should be registered by hostname. See [Registration](#).

View devices

There are many options for viewing devices that have been added to FortiNAC.

- **Inventory:** Displays lists of devices on the left side. When a device is selected, the right pane displays known information about that device with a graphic representation of device ports and connections. See [Inventory on page 289](#).

- **Host View:** Displays rogues or unknown devices and any devices that were manually registered and configured to display in Host View. See [Hosts on page 213](#).
- **Dashboard:** Host Summary and Device Summary panels provide totals for each device type broken down by status. See [Host Summary on page 89](#) and [Network Device Summary on page 93](#).

Learning about hosts on the network

When a host is on the network, FortiNAC needs to know that the host has connected or disconnected and what that host's IP address and MAC address are.

FortiNAC can learn this information in several ways including:

- Link up/link down traps sent by the switch
- MAC learned traps sent by the switch with the MAC address
- Polling network devices

See [SNMP trap support](#) for a list of currently supported traps.

Link up and link down traps

If a device on the network supports link up and link down traps, you should enable this feature and configure the device to send traps to the IP address of the FortiNAC Server or FortiNAC Control Server. As soon as the device is modeled in FortiNAC, FortiNAC listens for traps from that device. When FortiNAC receives a Linkup trap, it polls the switch to read the available host information. If FortiNAC does not receive information from the device after the first poll, it retries up to seven times.

Polling triggered by traps is configured from **System > Settings > Network Device**. The Minimum Trap Period (Sec) field controls the number of seconds FortiNAC waits after receiving a linkup trap before reading the forwarding table from the switch associated with the trap. The default is 10 seconds. The Max Number of Trap Periods field controls the number of periods FortiNAC waits before reading the forwarding table on the switch. The default setting for this field is 4. The number of retries is not configurable. See [Network device on page 910](#).

If you use link up traps, the process for learning that the host is connected and its MAC address and IP address is as follows:

1. A host connects to a switch.
2. The switch sends a link up trap to FortiNAC.
3. Assuming that the Minimum Trap Period is set to 10 seconds and the Max Number of Periods is set to 4, then FortiNAC waits 40 seconds to read the forwarding table on the switch.
4. If the host's MAC address is not returned, FortiNAC waits another 40 seconds and reads the forwarding table on the switch again. FortiNAC repeats this process up to seven times until it retrieves the host data.
5. If after seven retries the host data is not retrieved, FortiNAC does not try any more until the next scheduled poll for the device.

It is possible for a trap to be sent from the device and not be received by FortiNAC. Therefore, in addition to traps it is important to configure polling intervals in FortiNAC for each of your devices. Configuring polling is particularly important for wireless devices because it is the method used to determine that a host has disconnected from the wireless device. See [L2 polling on page 449](#) and [L3 polling on page 451](#).

MAC notification traps

MAC Learned or MAC Notification Traps are traps that send host information when the host connects or disconnects alleviating the need for FortiNAC to poll. These traps are only supported on some devices, such as Cisco switches. If MAC Notification traps are available and supported by FortiNAC for the device, it is beneficial to enable them and reduce network traffic created by frequent polling. To use MAC Notification Traps they must be enabled on the device and configured to be sent to the IP address of the FortiNAC Server and the device must be modeled in FortiNAC.

If you enable MAC Notification or MAC Learned traps on a device, you should disable Link Up and Link Down traps. They are redundant, cause additional traffic and prevent the MAC Learned event messages from being generated on FortiNAC.

If MAC Notification traps configured on Cisco devices are not being processed, verify the following: The SNMP user credentials entered in FortiNAC are for a User who is a member of a SNMP Group on the device. That the SNMP Group is configured with the contexts the group needs to access. Below is an example from a running configuration on a Cisco device:

```
snmp-server group testv3 v3 auth write view2
snmp-server group testv3 v3 auth context vlan-35
snmp-server group testv3 v3 auth context vlan-85
```

Polling

FortiNAC has a built in polling mechanism that compensates for missed traps or devices that are not configured to send traps by reading tables on network devices and retrieving host information. There are two types of polling used to gather host information:

- Layer 2 (L2) polling - FortiNAC reads the network device's MAC address table. This provides FortiNAC with the host's MAC address, switch and port location on the network.
- Layer 3 (L3) polling - Applies to Layer 3 network devices only. FortiNAC reads the network device's ARP table. This provides FortiNAC with the IP address that corresponds to the host's MAC address.

Polling information is stored for each device individually including: Enable/Disable Polling, Polling Interval, Last Successful Poll Time and Last Attempted Poll Time. For L3 devices Polling Priority is also stored.

Using the polling interval and the Last Successful Poll information stored for the device, FortiNAC polls devices individually. For example if device A has a polling interval of 15 minutes and a Last Successful Poll time of 10:15, then the next poll happens at 10:30 regardless of when other devices are being polled. The Last Successful Poll Time is updated any time the device is read, including using the Poll Now option or when a trap triggers FortiNAC to read the device. Updating Last Successful Poll Time for each contact with the device prevents unnecessary polling.

The Polling interval on devices is set initially based on device media type (wired or wireless). When network devices are discovered, they are analyzed and placed in groups. L2 devices are automatically placed in either the L2 Wired Devices or L2 Wireless groups. The default polling interval is 10 minutes for wireless devices and one hour for wired devices. Polling on wireless devices is more frequent because it is the only method for determining that a host has disconnected from the wireless device.

A default L3 (IP --> MAC) group is created by FortiNAC. During discovery this group is not automatically populated. You must add your L3 devices to this group.

See [L2 polling](#) and [L3 polling](#).

Isolate unknown devices

When any device connects to the network FortiNAC checks to see if it is registered or not. Registered devices are allowed to access the production network. Unregistered or unknown devices are placed in an isolation VLAN. There is some configuration required to isolate unknown devices.

VLANs

Make sure that you have at least one isolation VLAN where unknown devices can be placed until they are registered. Typically this is called the Registration VLAN. The condition for being placed in the Registration VLAN is that the device be unknown.

VLANs should also be configured on each switch or controller. VLANs should be read from the switches and included in the model configuration for each switch. See [Network access/VLANs on page 319](#) and [Model configuration on page 338](#).

Forced registration group

Ports that will be used to access your network should be placed in the Forced Registration Group. Placing ports in the Forced Registration Group, indicates to FortiNAC that unregistered devices connecting on those ports must be placed in the Registration VLAN to be isolated until the device is registered. For instructions on placing ports in this group

Control access based on device types

Depending on the demands of your organization you may need to limit device access to the network by time of day or by the type of Device. You may need to alter device parameters, such as baud rate or setting up traps, based on the type of device and where it is connecting.

Disable devices with scheduled tasks

To disable ports or adapters based on time of day use the Scheduler to create Scheduled Tasks that act on groups of ports or devices. The Scheduler associates tasks with groups. Therefore, either the affected ports must be placed in a port group or the affected devices must be placed in a host group. Only those devices that have been registered and configured to display in the Host View can be included in a host group. Since disabling ports blocks all network access, it is recommended that you disable the adapters of the devices that should be denied access to the network. For additional information, see [Add groups on page 845](#) and [Add a task on page 858](#).

Modify device settings

FortiNAC has the ability to store and use sets of CLI commands called CLI configurations. These command sets can be very powerful when managing devices and have several implementation options. CLI configurations can be implemented:

- By using the Scheduler to complete a task, such as setting up Link up/ Link down traps on a series of switches.
- By the role assigned to the device and the port on which it connects. For example, you could alter the baud rate of a medical device when it connects to the network.
- Through the model configuration of the switch to control VLANs or to implement ACLs that control connecting devices.

See [CLI configuration on page 433](#) for additional information.

Role based access

Every device in FortiNAC is assigned a role of NAC Default as it registers. Additional roles can be created and assigned to devices that require network services, such as printers. Only those devices that have been registered and configured to be managed in Inventory can use role-based access. Ports or switches must be placed in Port or Device groups. For example, if you have a role called Accounting, you can map that role to devices in with role X. Then indicate that when a device in with role X connects to the network through a switch or port in group Y, that device can only access VLAN 10. See [Roles on page 620](#) for detailed instructions.

View logs and reports

As devices register, and connect and disconnect from the network data is collected for all of those transactions. In addition events and alarms are generated depending on the activities of the device. Logs and reports that display device activity include the following:

- **Events View:** Displays a chronological list of events generated by device activity on the network. Each event contains data pertaining to the device that triggered the event, such as IP address or MAC address. See [Events on page 749](#).
- **Network Events:** Displays the connection log of users and hosts that have connected to the network. See [Connections view on page 1](#).
- **Reports View:** Provides access to standard reports and allows you to create custom reports based on the information in the database. The report data may be output to HTML, CSV, EXCEL, XML, RTF, and PDF formats.

Netflow Support

FortiNAC can leverage Netflow records for Device Profiling and supports the following: Netflow v5, v9, and v10 (IPFIX).

Requirements:

- Enable Netflow on the network device
 - Export destination = IP Address of FortiNAC
 - Listener port = 2055
- FortiNAC-OS Requirement: "set allowaccess" command option "netflow". See [Open ports](#) for details.

To view the information collected, go to Users & Hosts > Network Sessions. For more information, see [Network sessions](#).

To use in a profiling rule, utilize the Network Traffic Method as described in [Adding a rule on page 264](#)..

DNS configuration

The FortiNAC Server and FortiNAC Control Server appliances use Common Object Request Broker Architecture (CORBA) to communicate between the web server and the browser. Within the FortiNAC Server and FortiNAC Control Server appliances, CORBA uses the sub-domain or hostnames (short names), not IP addresses, to communicate between the browser and server. The administrator's host and the FortiNAC Server and FortiNAC Control Server appliance hostname must be in DNS.

If DNS is not available, then each administrator's host must have a host entry for the FortiNAC Server and FortiNAC Control Server appliances.

If you have security enabled, you cannot use the fully qualified domain name (FQDN) of the FortiNAC Server or FortiNAC Application Server. You must use the short name instead. If the FQDN is used and the administrator's host is using the Persistent Agent, the agent cannot communicate with the FortiNAC appliances. This could prevent the Administrator from registering the host.

The 'nac' alias must not be included in DNS. For example, do not use an alias like "nac.abc.def.com" anywhere in DNS.

Windows

1. Edit the `hosts` file on the system. The hosts file is usually in the following directory:
`C:\windows\system32\drivers\etc\hosts`.

2. Add this entry to the Hosts file:

```
XXX.XXX.XXX.XXX Short_Name
```

or

```
XXX.XXX.XXX.XXX host_name
```

Example:

```
192.168.10.1 qa233
```

3. Reboot the computer after you change the `hosts` file.

Having multiple interfaces on the Administrator workstation can sometimes cause DNS problems, depending on the interface configuration settings.

Sample Windows hosts file

```
# Copyright (c) 1993-1999 Microsoft Corp.
```

```
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to hostnames. Each entry
# should be kept on an individual line. The IP address should be placed in the first
# column followed by the corresponding hostname followed by the short name.
# The IP address, the hostname, and the short name should be separated by
# at least one space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the hostname denoted by a '#' symbol.
#
# For example:
#
# XXX.XXX.XXX.XXX host.domain.com # source server
# XXX.XXX.XXX.XXX host_name # x client host

127.0.0.1 localhost
```

Linux

1. Edit the `hosts` file on the system. The hosts file is usually in the following directory: `/etc/hosts`
2. Add this entry to the Hosts file:

```
XXX.XXX.XXX.XXX Short_Name
```

Example:

```
192.168.10.10 qa233
```

There is no need to reboot the system.

macOS

1. Locate the file named `hosts` in `/etc` folder.

If the file does not exist, create one with a text editor. The hosts file contains information regarding the known hosts on the network.

Separate the entries on each line with tabs. Do not use spaces. A `#` indicates the beginning of a comment; characters up to the end of the line are not interpreted by routines which search the file.

Use a single line for each host file. Make sure each host line contains the Internet address of the host, the fully qualified hostname, and the Alias.

Example:

```
xxx.xxx.xxx.xxx Qualified_Host_Name Alias
```

2. Reboot the computer after you have edited and saved the hosts file.

IPv6 support

FortiNAC has the ability to support IPv6 addresses by allowing IPv6 endstations (hosts, devices) to communicate with FortiNAC's Portal and Agents. The admin UI also supports both IPv4 and IPv6.

Network device management and discovery in Inventory requires networking equipment to have an IPv4 address.

Polling L3 (IP->MAC) data for devices is supported from the following vendors/switches:

- Cisco
- Juniper EX Switches
- HP ProCurve
- Brocade
- FortiGate

Please contact [Fortinet Support](#) to request additional device support.

IPv6 hosts and devices can communicate with the FortiNAC via Portal and Agents. Both port2 and port1 support IPv4 and IPv6, enabling IPv6 hosts and devices to access the Portal. When a host or device uses IPv6, the IPv6 address is displayed in the Host View or **Adapter View**, in addition to any IPv4 addresses associated with the host or device. The FortiNAC admin UI can be accessed using the IPv6 address assigned to port1.

Supported for IPv6	Not Supported for IPv6
Portal communication (port2)	Device management in Inventory (Creation/discovery of network devices)
Admin UI access (port1)	
Agent communication	
L3 polling	
IPv6 addresses displayed in the Host View and Adapter View	

Guided Install

This installation method option creates a series of Tasks that will help the user walk through the set up of the product to gain visibility as quickly as possible. The tasks are displayed in the **Pending Tasks** widget checklist. Each task is displayed and shows whether or not the task has been done. See [Pending Tasks](#) for details.

Guided Install is enabled during the initial connection to the FortiNAC GUI during setup. See [Config wizard](#).

Login procedure

The FortiNAC user interface is browser based. When you log in as an Administrator, you may create other administrators with an administrator profile.

There are different types of user records in FortiNAC: Standard users and Administrators. Administrators are users with Admin UI login access. System Administrator is a specific set of permissions. You can have more than one Administrator account with System Administrator permissions (Admin Profile).



There are no spaces in the entry. `<hostname>` is the name of the FortiNAC appliance. You may substitute the IP address for the `<hostname>` if you wish.

1. Enter one of the following URLs in the Address field of the browser window:
`https://<hostname>:8443/`
or
`http://<hostname>:8080/`
2. Log in as an administrator. Enter the **User Name** and **Password**.
3. The End User License Agreement appears the first time any administrator logs in. Click to Accept the terms. Clicking Disagree returns you to the Login dialog.
4. Add administrators as needed. See [Add an administrator on page 121](#) for instructions.
5. The FortiNAC user interface displays. The interface provides the appropriate privileges for whoever logs in. See [Administrator profiles on page 125](#) for more information on administrator permissions.

Connection errors

The table below contains a list of errors that could be displayed if you have problems connecting to the admin UI:

Message	Code	Definition
Unable to connect to host <hostname>	1050	Indicates that FortiNAC was unable to open the port and contact the server. Possible reasons include: Access could be blocked by a firewall. Java cache may need to be cleared. Hostname may be missing from the hosts file. See DNS configuration on page 26 for the location of the hosts file based on your operating system. Server may be down.

Licenses

The license key installed on your FortiNAC controls both the feature set that is enabled and the number of managed hosts, users and devices.

License types:

- **Plus:** Host registration, scanning, and access control.
- **Pro:** Automated Threat Response, along with all plus features.

All licenses include high availability.

License count

There are two types of license counts on FortiNAC: concurrent licenses and Pro licenses. See license usage information on the [Dashboard on page 86](#) and [License management on page 983](#).

If you exceed your license count, FortiNAC does the following:

- No new registrations are allowed.
- Attempts at new registrations are presented with the message **Exceeded concurrent connection license limit**.
- Rogues, at-risk, and disabled hosts continue to be placed in isolation as they normally would be.
- Existing registered hosts and devices continue to have network access.
- Network Access provisioning based on policy will not occur

Concurrent licenses

The count of concurrent licenses is based on the total number of concurrent connections to your network that are managed by FortiNAC. There may be parts of your network that are not managed by FortiNAC.

This count includes hosts, servers or devices that are online on your network at any given time. When a host, server or device disconnects from the network, the license is released and can be used for another connection. For example, you may have 1000 hosts in your database but if only 100 are connected, then only 100 licenses are used.

A registered host will use a license if the host is seen by FortiNAC to be online, even if the host is not on an enforced port. When a registered host shows online, even if no one is logged on, a license is still used. When the licenses run out, no new devices can register and access the network.

The following devices use a concurrent license when connected:

- Online hosts in the Host View (including registered hosts and IP phones)
- Online, non-infrastructure devices in Inventory (servers, printers, IP phones)

The following devices don't use a concurrent license when connected:

- Rogue devices
- Switches, routers, wireless controllers and wireless access points in Inventory

Pro licenses

These licenses are based on the total number of licenses configured that are currently in use by devices connected to your network.

Entitlements

Additional services at no cost come with licenses and are shown as entitlements in the license dashboard.

Entitlement	Description
Telephone Support	Global toll-free technical support available 24/7 over telephone.
IoT Detection	Access to database of devices through the cloud-look up service hosted by FortiGuard Labs used by FortiNAC to identify devices.
Vulnerability Management	Vulnerability analysis and remediation for potential security weakness.
Firmware & General Updates	Firmware updates and weekly network device database updates to keep deployments up to date.
Enhanced Support	24/7 FortiCare Enhanced Support that includes real-time ticket system, interactive chat features, and return/replace hardware support.

Events and alarms

When the number of licenses used reaches 75%, 95% and 100% of total licenses an event is generated for each threshold and an alarm is triggered to warn you. These percentages are default values. Modify thresholds for these events under Event Management. See [Event thresholds on page 774](#) for instructions.

Administrators must either monitor the **Security Alarms** view or the **Alarm** panel, or modify these alarms to send a notification to administrators as they occur.

Event	Definition
Maximum Concurrent Connections Warning	Concurrent licenses in use has reached or exceeded 75% of total licenses. Threshold is configurable.
Maximum Concurrent Connections Critical	Concurrent licenses in use has reached or exceeded 95% of total licenses. Threshold is configurable.
Maximum Concurrent Connections Exceeded	Concurrent licenses in use has reached 100% of total licenses.
Entitlement Polling Failure	(Requires version 8.8.10, 9.1.4, 9.2.0 or above) Generated when there is an error communicating or processing license entitlements data from Forticloud over TCP 443. Entitlement polling is required for Subscription Licenses. Refer to the Deployment Guide in the Document Library for Open Port requirements.
Entitlement Polling Success	(Requires version 8.8.10, 9.1.4, 9.2.0 or above) Generated when communication and processing of license entitlements data from Forticloud successfully completes.

Licenses are not released until users, hosts, devices or guests are disconnected from the network.

FortiNAC Manager

Licensed features

In a FortiNAC Manager environment, each appliance has its own license key that works in combination with the license on the FortiNAC Manager. Licensed features, such as device profiler, integration suite, guest manager, and endpoint compliance, can be enabled for all managed appliances by including the feature in the license key for the FortiNAC Manager. To enable a licensed feature on a single appliance, the feature must be included in the license key for that appliance, but must not be included in the FortiNAC Manager license key.

License totals

License counts are shared across all managed FortiNAC appliances, but the maximum number of licenses is controlled by the FortiNAC Manager.

For example, if the total number of concurrent connection licenses on the FortiNAC Manager is 1000, any of the managed appliances can use licenses from that pool, until all 1000 have been consumed. Appliance A may use 200 and Appliance B may use 150, leaving 650 available. Dashboards for all appliances, including the FortiNAC Manager, would display the following:

- Total Licenses: 1000
- Licenses In Use: 350
- Licenses Available: 650

Total licenses available and total licenses used are counted by the FortiNAC Manager and are displayed on the dashboard of all appliances.

Any number of licenses can be used on any managed appliance as long as total for all combined does not exceed the 1000 licenses configured on the FortiNAC Manager. This affects concurrent connection licenses.

In a multi-FortiNAC Server environment, a host that is connected to both wired and wireless FortiNAC Servers will use two licenses.

If the FortiNAC Manager goes down, individual FortiNAC Servers will continue to use the license counts.

License accounting for users and hosts

When users and their corresponding hosts move from one part of the network to another the FortiNAC appliance managing their network access may change. For example, if the switches on the first floor are managed by FortiNAC Appliance A and the switches on the second floor are managed by FortiNAC Appliance B, then network access control changes from Appliance A to Appliance B when a laptop is moved from the first floor to the second floor.

Hosts consume licenses when they are connected to the network. When a host is moved the license is released when the host disconnects. The same host consumes a license the next time it connects to the network regardless of where it connects.

License accounting for devices

When devices are moved from one part of the network to another the FortiNAC appliance managing their network access may change. If moving the device causes it to be managed by a different FortiNAC appliance, one license is released on the original appliance when the device disconnects from the network and then a new license is used when the device reconnects to the network. The device is included in the databases of both appliances but only consumes one license because it only has one connection.

Evaluation license keys

Evaluations license keys provide access to FortiNAC for a limited number of days allowing you to evaluate the system without purchasing a full license. Time is counted based on the amount of time the system has been running. When the system is shut down and restarted the time count continues from where it left off until the time limit is reached.

View time remaining

1. Select **System > Settings**.
2. In the tree and select **System Management**.
3. Select **License Management**.
4. Click **View**.
5. Verify the data in the **Evaluation Time** field. This field displays the number of days configured for the evaluation license. If you are not using an evaluation license, the **Evaluation Time** field does not display.

Installing a new key

1. If your evaluation license key has expired you are notified when you try to log into FortiNAC. The following message is displayed on the login window: **Your Evaluation License has expired**.
2. Request a new key from your sales representative.
3. Click **Enter New Key** to start the configuration wizard and apply the new key.
4. Click the **Enter New Key** link.
5. Enter the configuration wizard credentials.
6. The **License Key Validation** window is displayed.
7. Paste the text of the new license key into the **License Key** field.
8. Click **OK** at the bottom of the **License Key Validation** window.
9. Close the Configuration Wizard and log into FortiNAC.

Note: After FortiNAC version 7.6.5, a 3-day grace period for licenses expiration date will be added for ITF license.

Navigation tips

The section gives you some tips on how to use FortiNAC's GUI.

Filters

The Filter section can be opened or closed using the + and: symbols in the title bar of a page, for example **Network > L3 Polling**. Wild card characters can be used in text based fields.

Using filters

1. Navigate to a view that has a filter panel at the top.
2. Click in the **Add Filter** field and select a data type to use as a filter, such as **Host Name**.
3. A field is displayed for the data to be used as a filter. Enter the appropriate filter data.
4. Continue adding filter fields and filter data as needed.
5. Click **Update** to display the filtered data in the table.
6. To remove a filter, click the - symbol next to the field. Click **Update** to refresh the data in the table.

Filter types

Each view that has filters has options that are specific to that particular view. For example, Guest Contractor Accounts allows you to filter by account type. However, there are some filter options that are common to any views. The table below lists filters that are common across many views. Detailed filter information is available in the Help for each individual view.

Type	Definition
Time	Filters that involve date and time: • Last: Searches for timestamps within the last X number of minutes, hours or days by counting backwards from the current date and time. • Between: Searches for timestamps between the Start and End time - entered in YYYY/MM/DD hh:mm AM/PM format. • Month: Searches for timestamps between the month's start and end dates. For example, if March is selected, the filter searches for timestamps between 03/01/2015 00:00:00 and 03/31/2015 23:59:59. • After: Searches for timestamps after the Start time entered in YYYY/MM/DD hh:mm AM/PM format. • Before: Searches for timestamps before the Start time entered in YYYY/MM/DD hh:mm AM/PM format. Use Calendar to select a date.
Enabled	• Enabled: Record is enabled, such as a guest account. • Disabled: Record is disabled, such as a guest account.
Host Type	• Registered: Search includes only registered hosts or devices. • Rogue: Search includes only rogue or unregistered hosts or devices.
Authentication Type	• Local: Validates the user to a database on the local FortiNAC appliance. • LDAP: Validates the user to a directory database. FortiNAC uses the LDAP protocol to communicate to an organization's directory. • RADIUS: Validates the user to a RADIUS server.

Type	Definition
IP address	IP address of the connecting host or device.
Physical Address	MAC address of the connecting host or device.
Location	Name of the device and port where the host or device connected.
Group	Name of the group containing that contains devices, ports, users or hosts.
Container	Name of the Container in which a device is a member.
Registered	Shows Registered and Unregistered Hosts

Wild cards

When searching using a text field you must enter specific search data, such as 192.168.10.5. Wild cards can be used in these fields. Possible wild cards include the following:

Option	Example
*	192.* in the IP address field searches for all IP addresses that begin with 192.
[...]	[192.168.10.10,172.168.5.22,192.168.5.10] Searches for each IP address in the series and returns multiple records. Any search field that starts and ends with square brackets "[" and has one or more commas "," is treated as a list of values.
!	!192. in the IP address field searches for all IP addresses that do not contain 192.
![...]	![John, Frank, Bob] in the First Name field returns all records that do not contain John, Frank or Bob in the First Name field.
![...]	![Windows] in the operating system field returns all records that do not contain Windows in the operating system field.
<esc>!	<esc>!John in the First Name field returns records that match !John. The "<esc>" allows you to search for data that contains an exclamation point (!).
<esc>!	<esc>!Windows in the operating system field returns records that match !Windows. The "<esc>" allows you to search for data that contains an exclamation point (!).

Dashboard search

The search bar at the top of the dashboard can be used to search for any text, such as an IP address, a MAC address, or a word.

The results displayed can be one of three possible Result Types:

- Views (Pages)—Displays screens in the UI containing the searched item, such as Network Sessions, Administrators, etc. Clicking the result redirects to the screen where the searched item is listed.
- Settings—Displays the settings view that contains the searched item, such as System Settings, User Settings, Network Settings, etc. Clicking on the result redirects to the Settings screen where the searched item is listed.

- **Host Records**—Displays results for any host record containing the searched item. Clicking on the result redirects to **Users & Hosts > Hosts** and displays the matching host record found.

If one or more Result Type filters are enabled in the left column, only those results will display. If no filters are enabled, all results are displayed.



There is another type of search within the features themselves, for example **Network > L2 Polling**, that allows you to perform specific searches within the desired feature.

The Search tool will display **Recent Searches** and **Frequent Searches** done by the user. These can be clicked on to auto fill the search bar.

Quick search

Sometimes you have the option to search within a feature, for example in **Users & Hosts > User Accounts**. This is different from the dashboard search. If, for example, in User Accounts there are several accounts, the search function will appear to help you sort through them.

To use the quick search option:

1. Select **Users & Hosts**.
2. Select either the **Adapters**, **Hosts**, or **Users** tab.
3. Enter a single piece data in the search field and press **Enter**. Wild card searches can be done.

Quick search allows you to search based on a single piece of data, such as IP address, and display all matching records. To search by MAC address you must use one of the following formats:

```
xx:xx:xx:xx:xx:xx
xxxxxxxxxxxx
xx.xx.xx.xx.xx.xx
xx-xx-xx-xx-xx-xx
xxxx.xxxx.xxxx
```

Wild card searches can also be done. If you are doing a wild card search for a MAC address you must include colons as separators, such as 00:B6:5*. Without the separators the search option cannot distinguish that it is a MAC address.

If you are searching by IP address, you enter 192.168.5.1* and all records for IP addresses beginning with 192.168.5.1 are returned.

To broaden the search, enter less information, such as *11*. This returns any User Name, user ID, IP, MAC, or host name containing 11 depending on the tab you have selected.

Custom filter

The custom filter is the equivalent to an advanced search feature. It provides many fields that can be used in combination to narrow the list of Users, Adapters or Hosts displayed. A custom filter can be created and used just once or can be saved under a filter name.

Saved filters display in the drop-down menu and are separated into two sections:

- Private: Only the current user can see them
- Shared: Filter is shared with all administrators

They can be accessed by clicking the arrow on the quick search field at the top of the window. Custom filters can be modified, copied or deleted as needed. You can also export custom filters to a .txt file which allows custom filters to be imported and used by other administrators.

Use your mouse to hover over a saved filter in the drop-down menu and display a tooltip with details about that filter. There is currently only one default custom filter, Online Hosts, that displays a list of hosts that are connected to the network.

Create and save a custom filter

1. Select **Users & Hosts > Hosts**.
2. Select either the **Adapters**, **Hosts**, **User Accounts**, or **Applications** tab.
3. Click the arrow on the right side of the **Quick Search** field at the top of the window.
4. From the drop-down menu select **New Filter**.
5. Enter the name of the new filter.
6. Select the desired filter type (Private or Shared).
7. Click **OK**.



Filter names do not support more than 20 characters.

Continue with the topic below to configure the filter.

Configure a custom filter

This window is used in two ways. First if you have selected New Filter from the menu off of the quick search drop-down, you can configure the filter and FortiNAC saves it for future use. Second, if you have selected custom filter from the menu off of the quick search, you can configure this filter and use it just one time.



This dialog box is common to the adapter, host, and user views. Custom filter entries on any of these tabs will persist if you navigate between these views.

1. Once you have the Filter window displayed, enable the fields to be included in the filter by marking them with a check mark.
2. For each enabled field you must provide additional information. For example, if you select the Connected field, you must choose either On Line or Off Line.
3. For text fields, such as the IP address field, you must enter the search data, such as 192.168.10.5. Wild cards can be used in these fields.
4. To erase all selections, click **Clear All**.
5. If you have opened a saved filter and started to modify it, use **Reset** to return the filter to its original settings.
6. Click **OK** to run the configured filter. If this filter was assigned a name, the settings will be saved.

7. Click **OK** again to save the filter.
8. Immediately after the filter is run, the filter name displays at the top of the view in the quick search field.
To modify the filter, click the **Edit** link to the left of the quick search field. This modifies the filter whether it was saved or just configured and run one time.

Shared Reports

Shared Reports are generated based on shared filter results and can be configured to run on a scheduled basis. Resulting reports are saved as .csv files in the /home/cm/report directory. They can be downloaded using WinSCP or similar program (specify SCP transfer protocol).

Create New Schedule

1. Modify an existing shared filter or create a new one.
2. At the top of the view, click New Schedule.
3. Select the desired columns to be included in the report
4. Click **OK**
5. Specify the Schedule Type, Repetition Rate and Next Scheduled time
6. Click **OK**
7. Click **OK** again to save filter

Scheduled reports are saved as a task under **System > Scheduler**. They can be run at any time by selecting the task and clicking Run Now.

Edit a custom filter

1. Select **Users & Hosts**.
2. Select either the **Adapters**, **Hosts**, **User Accounts**, or **Applications** tab.
3. Click the arrow on the right side of the **Quick Search** field at the top of the window.
4. On the drop-down menu locate the custom filter to be edited and click the pencil or edit icon to the right of the filter name.
5. When the Filter window displays, modify the filter as needed.
6. Click **OK** to save your changes.

Delete a custom filter

1. Select **Users & Hosts**.
2. Select either the **Adapters**, **Hosts**, **User Accounts**, or **Applications** tab.
3. Click the arrow on the right side of the **Quick Search** field at the top of the window.
4. On the drop-down menu, locate the custom filter to be deleted and click the red X to the right of the filter name.
5. When the confirmation message displays, click **Yes**.

Export a custom filter

1. Select **Users & Hosts**.
2. Select either the **Adapters**, **Hosts**, **User Accounts**, or **Applications** tab.
3. Click the arrow on the right side of the **Quick Search** field at the top of the window.
4. On the drop-down menu select **Import/Export**, and then click **Export**.
5. In the Export Filters dialog, select the filters you want to export. Use Ctrl or Shift to select multiple filters.
6. Click **OK**. The filters are downloaded to a .txt file to your default download directory.

Import a custom filter

1. Select **User & Hosts**.
2. Select either the **Adapters**, **Hosts**, **User Accounts**, or **Applications** tab.
3. Click the arrow on the right side of the **Quick Search** field at the top of the window.
4. On the drop-down menu select **Import/Export**, and then click **Import**.
5. Click **Choose File** to find and select the .txt file containing the filters.
6. Click **OK** to import the filters. The filters appears in the list.

CLI Console

FortiNAC CLI Console is available starting from FortiNAC 7.6.1. FortiNAC CLI console is accessible through admin GUI.

dev1-l3-11-fortinac72.nacqa.test >_ 🔔 ? 👤 admin

Endpoint Fingerprints Manual ↕ ↻ ⌂

Delete Set Source Rank

Rogue 7 Registered 0 Both

Physical Address	Device Type	Operating System	IP Address	Host Name
00:50:56:B5:F6:17	Network	FortiSwitch		S108DVOV2YTR
00:50:56:B5:F6:17	Network	FortiSwitch		S108DVOV2YTR
00:50:56:B5:E9:CF	Linux	Ubuntu	10.10.11.10	linux
00:50:56:B5:E9:CF			10.10.11.10	
00:50:56:B5:DE:48	Linux	Fedora based		
00:50:56:B5:4E:2B	Windows	Windows XP/2000 (R...	10.10.11.11	

0% 12 | Updated: 15:09:29 ↻

The CLI user account and GUI admin account are separated, you will be asked to log in again with your CLI user account credential.

>_ Terminal

```
dev1-l3-11-fortinac72 login:
```

See [CLI Reference Manual](#) for more details on commands.

Wild cards

When searching using a text field in a custom filter or the quick search field you must enter specific search data, such as 192.168.10.5. Wild cards can be used in these fields. Possible wild cards include the following:

Option	Example
*	192.* in the IP address field searches for all IP addresses that begin with 192.
[...]	[192.168.10.10,172.168.5.22,192.168.5.10] Searches for each IP address in the series and returns multiple records. Any search field that starts and ends with square brackets "[" and "]" and has one or more commas "," is treated as a list of values.
!	!192. in the IP address field searches for all IP addresses that do not contain 192.
![...]	![John, Frank, Bob] in the First Name field returns all records that do not contain John, Frank or Bob in the First Name field.
<esc>!	<esc>!John in the First Name field returns records that match !John. The "<esc>" allows you to search for data that contains an exclamation point (!).

Find containers or devices

When you select **Find** a search field opens, allowing you to search for Containers or Devices. Search options include the following:

- Container Name
- Device Name
- Device IP address
- Device MAC address

When text or numbers are entered in the search field, FortiNAC searches for anything in the Inventory containing that text. For example, if you entered Com in the search field, FortiNAC would find the device named 3Com4330. Find is case sensitive and wild cards cannot be used.

Download logs

Logs can be downloaded to the client via a "Download Logs" menu item available under the help drop down in the top right of the GUI.

An advanced button in the menu opens a configuration view that allows for advanced log download configuration to:

- Select other servers (HA/FortiNAC Manager)
- Optional zip pwd
- File type (ZIP/Tar-GZIP/Tar-XZ)

Passwords

There are several types of passwords that are used in conjunction with FortiNAC, such as passwords for CLI, SSH, or admin UI access. Each type of password has its own set of rules or conventions.

CLI/SSH passwords

Passwords are set using the Guided Install during initial configuration.

Modify CLI Account passwords after initial configuration.

Login as admin to the CLI and type:

```
config sys admin
edit admin
set password [<password>]
end
```

For additional details on editing the Admin user(s) in the FortiNAC-OS CLI, see Admin user in the [CLI Reference manual](#).

CLI/SSH passwords must be eight characters or longer and contain a lowercase letter, an uppercase letter, a number, and one of the following symbols:

Required Symbols		
! exclamation point	@ at	_ underscore
# pound	\$ dollar	~ tilde
^ caret	- hyphen	* asterisk
% percent	? question mark	

The symbols listed below are not permitted in CLI/SSH and Configuration Wizard passwords.

Prohibited Symbols		
(open parenthesis	; semicolon	{ open curly bracket
) close parenthesis	: colon	} close curly bracket
' back quote	" double quote	[open square bracket
& ampersand	' single quote	] close square bracket
+ plus	< less than	, comma
= equal	> greater than	. period
pipe	\ back slash	/ forward slash

Admin CLI and root CLI passwords are limited to 64 characters.

Administrator passwords

To modify Administrator passwords, navigate to **Users & Hosts > Administrators**.



Spaces are permitted in passwords with local authentication. Any other authentication will depend on the vendor.

Administrator passwords for FortiNAC stored in the FortiNAC database must conform to the following:

Permitted Characters

Letters (upper and lower case)	A, B, C... (and a, b, c...)
Numbers	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Symbols	All characters not defined as letters or numbers. Including: ~!@#\$%^&*()_+ - = { } [] \ : < > ? , . /

Prohibited Symbols

' single quote	" double quote

Time stamps and time zones

Time for both the display and the database is stored in Coordinated Universal Time (UTC) and is adjusted based on the time zone setting in your browser. UTC corresponds roughly to Greenwich Mean time. Therefore, if the time zone for your browser is set to Eastern Standard Time, the program subtracts five hours from UTC time as it prints and displays the date and time for you.

Database

In the database, time is stored in UTC time, but the raw data is stored using a Unix convention. Date and time are represented as a Unix timestamp: the number of seconds elapsed since 1 January 1970 00:00:00 Greenwich Mean Time.

Display and export

Date and time are shown and exported as mm/dd/yy hh:mm AM or PM and time zone. For example the time stamp for a record could be 08/27/10 04:15 PM EDT.

Icons

Icons in FortiNAC represent different devices and users as they connect to and access the network. Host Icons are displayed in the Host View and the Inventory on the Ports tab. System Icons are displayed in the Inventory. Device Icons are displayed either in Hosts View, Profiled Devices, dashboard or Inventory depending on where they are being managed. Host Icons in particular have many states.

Icons in FortiNAC represent different devices and users as they connect to and access the network. Host Icons are displayed in the Hosts View. Device Icons are displayed either in Hosts View or the Device Summary Panel on the dashboard. Host Icons in particular have many states.

To indicate the state of a user, a device or a host, the icons are modified slightly by superimposing an image on top, such as a red box to indicate that the item has been disabled. States can be cumulative. For example, you could see an "X" over a host icon. This indicates that the host has been disabled but is still online. The table below provides a legend for those states.

Icon state

State	Definition	State	Definition
Hosts, adapters or users view			
	Online / Enabled: No image over icon indicates that the item, such as a Host or Adapter is online.		Offline / Enabled: Icon pixelated indicates that the item, such as a Host or Adapter is offline.
	Online / Disabled: Host or User was disabled but is online. This could be due to a misconfiguration of a switch or port or because the host was online at the time it was disabled. Defined as a Violation in some summary windows.		Offline / Disabled: Host or User is disabled and is not online.
	Go To: Allows you to select an icon on the user, host or Adapter View and navigate to corresponding information on another view. For example, if you have a host selected on the Host View, and you click the Go To on the Adapter icon, the Adapter View is displayed with the appropriate adapter selected.		Offline Device: A device being managed through the Host View is not connected to the network, such as a gaming device or an IP phone.
	Not Authenticated: Located at the upper-left corner of the icon. User has not yet authenticated. There is a delay between when the user's computer is connected to the network and when it is placed in the authentication VLAN.		Security Risk: Located at the upper-right corner of the icon. Host has been moved to remediation.

State	Definition	State	Definition
+	Pending At Risk: Located at the upper-right corner of the icon. Host has failed a scan that is set to delayed remediation for x number of days. Icon indicates that the host has not yet been marked "at risk" but will be after the delay set in the scan has elapsed.	   	- Persistent Agent not installed - Persistent Agent installed and communicating - Persistent Agent installed and not communicating
Inventory			
	No image over icon=Contact Established		Device Contact Unknown. Indicates that FortiNAC has not made initial contact with the device. Upon initial contact, FortiNAC queries the device and verifies the device type.
	Device Contact Lost		
  	Wireless switch Blue: Initial contact has not been made Red: Contact Lost Gray: Contact Established	  	Container Blue: Initial contact has not been made with one or more devices in the container Red: Contact lost with one or more devices in the container Gray: Contact established with all devices in the container
  	Port Admin status is on and Link status is up, indicating Host or device connected Admin status is on and Link status is down, indicating that nothing is connected Admin status is Off.		

The icons shown in the table below represent hosts, users and devices that are either online or in a good state, such as hosts that are Safe.

Icon list

Icon	Definition	Icon	Definition
Adapter, host and user icons			

Icon	Definition	Icon	Definition
	Adapter		Rogue Host
	Registered Host		IP Phone
	Contractor		Guest
	User		Administrator
System icons			
	Container		Multi Access Point (multiple hosts connected to one port, and none of the ports are phones)
	New Registered Host/Phone (one registered host and one phone are connected to a port)		New Rogue Host/Phone (one rogue host and one phone are connected to a port)
	New Cloud/Phone Icon Used when one of the following is true: More than one phone and one registered host connected to a port More than one registered host and one phone connected to a port More than one registered host and more than one phones connected to a port		Wired Port
	Link to a neighboring device		Process Plug-In
	Port Aggregate Uplink		SSID: Wireless Connection
	Directory		Process
Device icons			
	Alarm System		Android
	Apple Device		Camera
	Card Reader		Cash Register

Icon	Definition	Icon	Definition
	Dialup Server		Environmental
	Firewall		Gaming Device
	Generic Monitoring System		Health Care Device
	Hub		Internet TV
	IP Phone		IPS/IDS
	Linux		macOS
	Mobile or Apple iOS or Android		Generic Network Device
	PBX		Pingable Device
	Printer		Router
	Server		Switch
	Unknown Device		Unix
	UPS		Vending Machine
	VPN Connection	W	Windows
	Wireless Switch		

Certificates

SSL certificates can be used to secure many different types of connections for FortiNAC. The table below outlines the uses and requirements for these certificates.

Please note:

- Applies to all certificates imported into or saved on FortiNAC appliances.
- Certificates that use SHA2 encryption are not supported.

- Valid certificates are certificates that were obtained from a signing authority, such as VeriSign.
- Update the list of Allowed Domains with the domain of the certificate vendor. See [Allowed domains on page 907](#).
- Make sure that your network has a VLAN that allows hosts in isolation to access the internet when the host attempts to reach one of the sites in the Allowed Domains list.

It is recommended that you set the home page to a HTTP URL instead of a HTTPS URL to avoid receiving a certificate warning when opening your browser in IE while in the registration VLAN.

Connection	Types	Required	Format	Location	If no certificate
Admin UI	Self-Signed or Valid	No		/bsc/services	Works with or without a certificate.
Portal	Self-Signed or Valid	No	PEM	Imported	Works with or without a certificate.
Persistent Agent	Self-Signed or Valid	Yes Agent 3.0 or higher		Imported	Use agents lower than 3.0.
Dissolvable Agent	Self-Signed or Valid	Yes Agent 3.0 or higher		Imported	Use agents lower than 3.0.
Mobile Agent	Valid	Yes		Imported	No workaround, must use certificate.
LDAP Directory	Valid	No		/bsc/campusMgr	Do not select SSL or TLS protocols on the Directory Configuration view.
RADIUS Server	Valid	Yes with 802.1x and PEAP.		Proprietary	Use security options WEP, WPA or WPA2 , which use PSK, instead of the enterprise versions which use PEAP.
Supplicant Configuration	Valid	Yes for Windows hosts if RADIUS server has certificate and uses 802.1x and PEAP.	PEM or binary	Imported	Use security options WEP, WPA or WPA2 , which use PSK, instead of the enterprise versions which use PEAP. Or Windows hosts will have poor user experience with connection delays during supplicant configuration implementation.

Connection	Types	Required	Format	Location	If no certificate
Palo Alto Integration		Yes		N/A FortiNAC automatically imports from Palo Alto	Required

Associated certificate documentation

Connection	Topic
Admin UI	See SSL certificates on page 509 .
Portal	See Portal SSL on page 745 .
Persistent Agent	See SSL certificates on page 509 .
Dissolvable Agent	
Mobile Agent	
LDAP Directory	See Create a keystore for SSL or TLS on page 881
RADIUS Server	See the documentation for your RADIUS server.
Supplicant Configuration	See Supplicant EasyConnect on page 595 .
Palo Alto Integration	See Add or modify the Palo Alto User-ID agent as a pingable on page 304 .

Supported TLS Versions

For instructions on enabling and disabling TLS versions via the Administration UI, see TLS service settings under [Transport configurations](#) in the Administration Guide.

F 7.6

Admin UI	Enabled by Default: v1.2, v1.3 Configurable via GUI: v1.0, v1.1
Portal	Enabled by Default: v1.2, v1.3 (not configurable)
RADIUS EAP Methods Using TLS	Enabled by Default: v1.2, v1.3* Configurable via GUI: v1.0, v1.1 *v1.3 added to default setting in F 7.6.3. v1.3 was configurable via GUI in prior versions.
Persistent Agent	Enabled by Default: v1.2, v1.3 Configurable via GUI: v1.0, v1.1

Agent versions

9.4.4 Windows 10.7.2 Linux and macOS F 7.2 Android	Enabled by Default: v1.2, v1.3
F 7.6	Enabled by Default: v1.3 (v1.2 not supported)

Open ports

The FortiNAC software runs on top of the FortiNAC-OS operating system. For security purposes, FortiNAC-OS has minimal open (listening) TCP/UDP ports configured by default. The `set allowaccess` CLI command gives administrators the ability to configure FortiNAC to listen for unsolicited network communication over certain ports. The FortiNAC features used determine which ports need to be opened..

The best practice is to keep the number of open ports to a minimum and block all other ports. If you need to provide users access to network resources through a static port (e.g., from outside a firewall), the best option is to allow users to connect by VPN.

Related Documents

<http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>

Validate Open Ports

The current listening port configuration can be viewed by running an `nmap` of the appliance. Another useful command is `netstat` to list all listening and connected ports on the current appliance (e.g. `netstat -ln` lists just the listening ports).

Use the `netstat` command to verify that a TCP/UDP port is open.

FortiNAC CLI:

```
execute enter-shell
netstat -ln | grep <port number>
```

For example, use `netstat -ln | grep 4568` to verify that the port used for Agent communications to FortiNAC is open.

```
tcp 0 0 0.0.0.0:4568 0.0.0.0:* LISTEN
```

FortiNAC Open Port List

The following tables list ports that should be open to end users and ports that need to be open for FortiNAC communications:

[FortiNAC Access Configuration on page 51](#) - Available options for the `set allowaccess` command in the FortiNAC CLI.

[FortiNAC CA Firewall Policy Requirements on page 54](#) - Functionality specific to the ControlApplication Server (CA) and the required ports.

[FortiNAC Manager Firewall Policy Requirements on page 57](#) - Functionality specific to the Manager and the required ports.

[Fortinet Device Integration Firewall Policy Requirements on page 59](#) - Required ports based upon Fortinet device integrations (FortiGate, FortiSwitch, etc).

[Third Party Device Integration Firewall Policy Requirements on page 63](#) - Required ports based upon third party network device integrations.

FortiNAC Access Configuration

This table lists the available options for the `set allowaccess` command in the FortiNAC CLI. The `allowaccess` options are required to allow FortiNAC to listen to certain unsolicited inbound communication. The port specified is the FortiNAC interface on which the `allowaccess` option should be configured.

For a full list of available commands, refer to the FortiNAC CLI Reference Manual.

Related Feature/Function	Protocol & Port	set allowaccess Option	Configure FortiNAC Interface
PING is used to verify IP contact with FortiNAC port1 and port2	ICMP	ping	port1 port2
Remote CLI access	SSH (TCP port 22)	ssh	port1
Isolation scopes & Captive Portal	DHCP (UDP ports 67, 68, 546, 547) DNS (TCP/UDP port 53) HTTPS (TCP port 443)	dhcp dns https	port2
DHCP Fingerprinting	DHCP (UDP ports 67, 68, 546, 547)	dhcp	port1
Network Device Management	SNMP (UDP ports 161 and 162)	snmp	port1
Device Change Notification from IPS/IDS devices using syslog Endpoint Connectivity Notification using syslog (e.g. FortiGate)	Syslog (UDP port 53)	syslog	port1
High Availability FortiNAC Manager	TCP ports 1050, 5555, 9443, 18090, 30000-64000	nac-ipc	port1
Local RADIUS Virtual Server Proxy RADIUS Virtual Server (Authentication & Accounting)	RADIUS TCP/UDP port 1812 [default] - Authentication RADIUS TCP/UDP port 1813 [default] - Accounting	radius-auth radius-acct	port1
Local RADIUS Virtual Server (RadSec)	RADIUS (TCP port 2083 [default])	radius-radsec	port1
Legacy Proxy RADIUS (Authentication & Accounting)	RADIUS Legacy Proxy Authentication (TCP/UDP port 1645 [default]) RADIUS Legacy Proxy Accounting (TCP/UDP port 1646 [default])	radius-legacy-auth radius-legacy-acct	port1

Related Feature/Function	Protocol & Port	set allowaccess Option	Configure FortiNAC Interface
Persistent Agent	FortiNAC Agent (TCP port 4568)	nac-agent	port1 port2
Fortinet Single Sign-On	TCP port 8000	fsso	port1
Admin UI (TCP 8443)	HTTPS (TCP port 8443)	https-adminui	port1
Admin UI (TCP 8080)	HTTP (TCP port 8080)	http-adminui	port1
Network Sessions	NetFlow (UDP port 2055)	netflow	port1
Agent updates from FortiNAC	HTTP (TCP 80)	http	port1 & port2

FortiNAC CA Firewall Policy Requirements

This table lists functionality specific to the ControlApplication Server (CA) and the required ports.

The Direction column Indicates the direction the conversation is initiated with respect to FortiNAC.

- Outbound is initiated by FortiNAC. In such cases, response traffic should not be blocked.
- Inbound is initiated by another device and considered unsolicited.

Port	Protocol	Description	Direction
All ports outbound	All	Used by Device Profiler to classify devices. Uses NMAP as one of the profiling choices. Also can use SNMP to profile.	port1: Outbound port2: Outbound
	ICMP	PING (Optional)	port1: Bidirectional port2: Bidirectional
UDP/TCP 21	FTP	Product Updates (fnac-updates.fortinet.net)	port1: Outbound to internet
TCP 22	SSH	FortiNAC CLI Access	port1: Inbound
		Device Management (CLI access)	port1: Outbound
		Inter-Server Communication (High Availability)	Bi-directional between Primary and Secondary Server port 1
TCP 23	Telnet	Network Device Management	port1: Outbound port2: Outbound
TCP/UDP 53	DNS	FortiNAC queries production DNS server	port1: Outbound
		FortiNAC acts as DNS Server for Isolation Scopes	port2: Inbound
UDP 67 & 68	DHCP	DHCP Fingerprinting	(UDP 67) port1: Inbound & port2: Inbound
		Serving IP Addresses for Isolation Scopes	(UDP 68) port1: Inbound & port2: Outbound
UDP 547	DHCPv6	DHCP Fingerprinting	port1: Inbound
TCP 80	HTTP	Web Server (Portal)	port1: Inbound port2: Inbound
		Agent updates from FortiNAC	port1: Inbound port2: Inbound

Port	Protocol	Description	Direction
TCP 22	SFTP	Product Updates (fnac-updates.fortinet.net)	port1: Outbound to internet
UDP 123	NTP	Time Service	port1: Outbound
UDP 161	SNMP	Network Device Management	port1: Outbound (Bi-directional if FortiNAC is configured to respond to SNMP queries. See section SNMP of the Administration Guide).
UDP 162	SNMP	Traps for notifying FortiNAC of the following: Endpoint Network Connection changes Device Changes	port1: Inbound
TCP 443	HTTPS	Web Server (Portal) Secure HTTP	port2: Inbound
		Product Updates (fnac-updates.fortinet.net)	
		License Entitlements (fds1.fortinet.com globalupdate.fortinet.net)	port1: Outbound to internet
		FortiGuard - For details see Device Profiler IoT Query URL: globaldevquery.fortinet.net usdevquery.fortinet.net eudevquery.fortinet.net globaldevquery2.fortinet.net usdevquery2.fortinet.net eudevquery2.fortinet.net Collect URL (IoT Data Collection): globaldevcollect.fortinet.net usdevcollect.fortinet.net eudevcollect.fortinet.net globaldevcollect2.fortinet.net usdevcollect2.fortinet.net eudevcollect2.fortinet.net	
UDP 514	Syslog	Logging of events to external server (outbound)	port1: Bidirectional
TCP 1050 TCP 5555 TCP 9443 TCP 18090	CORBA	Inter-Server Communication (High Availability)	Bi-directional between Primary and Secondary Server port1

Port	Protocol	Description	Direction
TCP 30000-64000			
TCP 4568	Agent Server	Persistent Agent Communication	port1: Bidirectional port2: Bidirectional
TCP 5986 (default) User modifiable	WinRM	WMI profiling method	port1 and port2: Outbound
TCP 8443	HTTPS	Web Server Secure HTTP (Admin UI)	port1: Inbound
TCP 8080	HTTP Alternative	Web Server (Admin UI)	port1: Inbound
UDP 2055	NetFlow	Used to receive netflow data from network devices to populate the "Network Sessions" view in the Administration UI. See Network sessions for details.	port1: Inbound
TCP 8443	HA	For communication between the primary and secondary nodes.	port1: Inbound

FortiNAC Manager Firewall Policy Requirements

This table lists functionality specific to the FortiNAC Manager and the required ports.

The Direction column Indicates the direction the conversation is initiated with respect to FortiNAC.

- Outbound is initiated by FortiNAC. In such cases, response traffic should not be blocked.
- Inbound is initiated by another device and considered unsolicited.

Port	Protocol	Description	Direction
	ICMP	PING (Optional)	port1: Bidirectional port2: Bidirectional
UDP/TCP 21	FTP	Product Updates (fnac-updates.fortinet.net)	port1: Outbound to internet
TCP 22	SSH	FortiNAC CLI Access	port1: Inbound
		Inter-Server Communication (High Availability)	Bi-directional between Primary and Secondary Server port1
		Inter-Server Communication (FortiNAC Manager)	Bi-directional between Managed Servers and Manager port1
TCP/UDP 53	DNS	FortiNAC queries production DNS server	port1: Outbound
TCP 22	SFTP	Product Updates (fnac-updates.fortinet.net)	port1: Outbound to internet
UDP 123	NTP	Time Service	port1: Outbound

Port	Protocol	Description	Direction
TCP 443	HTTPS	License Entitlements (fds1.fortinet.com globalupdate.fortinet.net)	port1: Outbound to internet
		Product Updates (fnac- updates.fortinet.net)	
		FortiGuard - For details see Device Profiler IoT Query URL: globaldevquery.fortinet.net usdevquery.fortinet.net eudevquery.fortinet.net globaldevquery2.fortinet.net usdevquery2.fortinet.net eudevquery2.fortinet.net Collect URL (IoT Data collection): globaldevcollect.fortinet.net usdevcollect.fortinet.net eudevcollect.fortinet.net globaldevcollect2.fortinet.net usdevcollect2.fortinet.net eudevcollect2.fortinet.net	
UDP 514	Syslog	Logging of events to external server (outbound)	port1: Bidirectional
TCP 1050 TCP 5555	CORBA (1050, 5555)	Inter-Server Communication (High Availability)	Bi-directional between Primary and Secondary Server port1
TCP 9443 TCP 18090	gRPC (9443, 18090)	Inter-Server Communication (FortiNAC Manager)	Bi-directional between Managed Servers and Manager port1
TCP 8443	HTTPS	Web Server Secure HTTP (Admin UI)	port1: Inbound
		FortiNAC Manager (M): Manage FortiNAC Servers	Bi-directional between Managed Servers port1 and Manager port1
TCP 8080	HTTP Alternative	Web Server (Admin UI)	port1: Inbound

Fortinet Device Integration Firewall Policy Requirements

This table lists the required ports based upon Fortinet device integrations (FortiGate, FortiSwitch, etc).

The Direction column Indicates the direction the conversation is initiated with respect to FortiNAC.

- Outbound is initiated by FortiNAC. In such cases, response traffic should not be blocked.
- Inbound is initiated by another device and considered unsolicited.

Device Integration	Protocol	Port	Description	Direction	Allowaccess Option
FortiAnalyzer	Syslog	TCP 514	Logging of events to external server (outbound)	port1: Bidirectional	syslog
FortiAP Integration FortiGate Endpoint Management - FortiGate Wired Interfaces (RADIUS Optional) - FortiWiFi	RADIUS	TCP/UDP 1812 (default) User modifiable	Authentication	port1: Bi-directional	radius-auth
	RADIUS	TCP/UDP 1813 (default) authentication port value + 1	Accounting	port1: Inbound	radius-acct
	RADIUS	TCP 2083 (default) User modifiable	RADIUS over TLS (RadSec)	port1: Bi-directional	radius-radsec
	RADIUS	TCP 389	Winbind (MSCHAPv2 authentication)	port1: Outbound	N/A
	RADIUS	UDP 3799	Change of Authorization (CoA) or Disconnect	port1: Outbound	N/A
	HTTPS	TCP 443 (default or as defined on FortiGate)	REST API	port1: Outbound	N/A

Device Integration	Protocol	Port	Description	Direction	Allowaccess Option
FortiGate VPN	Private Protocol	TCP 8000	Fortinet Single sign-On (FSSO) communications	port1: Inbound	fsso
	Private Protocol	TCP 8013	Fortinet Security Fabric	port1: Inbound	N/A
	Syslog	UDP 514	Logging of events to external server (outbound)	port1: Bidirectional	syslog
	Agent Server	TCP 4568	Persistent Agent Communication	port1: Bidirectional port2: Bidirectional	nac-agent
	HTTPS	TCP 443 (default or as defined on FortiGate)	REST API	port1: Outbound	N/A

Device Integration	Protocol	Port	Description	Direction	Allowaccess Option
FortiSwitch FortiLink	RADIUS	TCP/UDP 1812 (default) User modifiable	Authentication	port1: Bi-directional	radius-auth
	RADIUS	UDP 3799	Change of Authorization (CoA) or Disconnect	port1: Outbound	N/A
	RADIUS	TCP 2083 (default) User modifiable	RADIUS over TLS (RadSec)	port1: Bi-directional	radius-radsec
	RADIUS	TCP 389	Winbind (MSCHAPv2 authentication)	port1: Outbound	N/A
	Private Protocol	TCP 8000	Fortinet Single sign-On (FSSO) communications	port1: Inbound	fsso
	Private Protocol	TCP 8013	Fortinet Security Fabric	port1: Inbound	N/A
	Syslog	UDP 514	Endpoint connection notification	port1: Inbound	syslog
	HTTPS	TCP 443 (default or as defined on FortiGate)	REST API	port1: Outbound	N/A

Device Integration	Protocol	Port	Description	Direction	Allowaccess Option
FortiSwitch Standalone	RADIUS	TCP/UDP 1812 (default) User modifiable	Authentication	port1: Bi-directional	radius-auth
	RADIUS	UDP 3799	Change of Authorization (CoA) or Disconnect	port1: Outbound	N/A
	RADIUS	TCP 2083 (default) User modifiable	RADIUS over TLS (RadSec)	port1: Bi-directional	radius-radsec
	RADIUS	TCP 389	Winbind (MSCHAPv2 authentication)	port1: Outbound	N/A
	HTTPS	TCP 443 (default or as defined on FortiGate)	REST API	port1: Outbound	N/A
FortiWLC Device Configuration	RADIUS	TCP/UDP 1812 (default) User modifiable	Authentication	port1: Bi-directional	radius-auth
	RADIUS	TCP 2083 (default) User modifiable	RADIUS over TLS (RadSec)	port1: Bi-directional	radius-radsec
	RADIUS	TCP 389	Winbind (MSCHAPv2 authentication)	port1: Outbound	N/A

Third Party Device Integration Firewall Policy Requirements

This table lists the required ports based upon third party network device integrations.

The Direction column Indicates the direction the conversation is initiated with respect to FortiNAC.

- Outbound is initiated by FortiNAC. In such cases, response traffic should not be blocked.
- Inbound is initiated by another device and considered unsolicited.

Device Integration	Protocol	Port	Description	Direction	Allowac- cess Option
Arista Cloud Wireless Aruba and Alcatel Wireless Controller Extreme/Motorola	RADIUS	TCP/UDP 1812 (default) User modifiable	Authentication	port1: Bi- directional	radius- auth
	RADIUS	TCP/UDP 1813 (default) authenticatio n port value + 1	Accounting	port1: Inbound	radius- acct
	RADIUS	TCP 2083 (default) User modifiable	RADIUS over TLS (RadSec)	port1: Bi- directional	radius- radsec
	RADIUS	TCP 389	Winbind (MSCHAPv2 authentication)	port1: Outbound	N/A
Aruba Instant AP Wireless Cambium AP Wireless ExtremeCloud/Aerohi ve Wireless Ruckus Smart Zone Ubiquiti UniFI Access Point	RADIUS	TCP/UDP 1812 (default) User modifiable	Authentication	port1: Bi- directional	radius- auth
	RADIUS	TCP/UDP 1813 (default) authenticatio n port value + 1	Accounting	port1: Inbound	radius- acct
	RADIUS	TCP 2083	RADIUS over TLS	port1: Bi-	radius-

Device Integration	Pro- to- col	Port	Description	Direction	Allowac- cess Option
		(default) User modifiable	(RadSec)	directional	radsec
	RADIUS	TCP 389	Winbind (MSCHAPv2 authentication)	port1:Outbound	N/A
	RADIUS	UDP 3799	Change of Authorization (CoA) or Disconnect	port1: Outbound	N/A
Cisco Meraki MS Switch Cisco Wireless Controller	RADIUS	TCP/UDP 1812 (default) User modifiable	Authentication	port1: Bi-directional	radius-auth
	RADIUS	TCP/UDP 1813 (default) authentication port value + 1	Accounting	port1: Inbound	radius-acct
	RADIUS	TCP 2083 (default) User modifiable	RADIUS over TLS (RadSec)	port1: Bi-directional	radius-radsec
	RADIUS	TCP 389	Winbind (MSCHAPv2 authentication)	port1:Outbound	N/A
	RADIUS	UDP 1700	Change of Authorization (CoA) or Disconnect	port1: Outbound	N/A
Huawei Wireless	RADIUS	TCP/UDP 1812 (default) User modifiable	Authentication	port1: Bi-directional	radius-auth
	RADIUS	TCP 2083 (default) User modifiable	RADIUS over TLS (RadSec)	port1: Bi-directional	radius-radsec
	RADIUS	TCP 389	Winbind (MSCHAPv2 authentication)	port1: Outbound	N/A

Device Integration	Pro- tocol	Port	Description	Direction	Allowac- cess Option
	RADIUS	UDP 3799	Change of Authorization (CoA) or Disconnect	port1: Outbound	N/A
Cisco Meraki MR Access Points	Syslog	UDP 514	Logging of events to external server (outbound)	port1: Bidirectional	syslog
	RADIUS	TCP/UDP 1812 (default) User modifiable	Authentication	port1: Bi-directional	radius-auth
	RADIUS	TCP 2083 (default) User modifiable	RADIUS over TLS (RadSec)	port1: Bi-directional	radius-radsec
	RADIUS	TCP 389	Winbind (MSCHAPv2 authentication)	port1: Outbound	N/A
	RADIUS	UDP 3799	Change of Authorization (CoA) or Disconnect	port1: Outbound	N/A
Generic Wired RADIUS	RADIUS	TCP/UDP 1812 (default) User modifiable	Authentication	port1: Bi-directional	radius-auth
	RADIUS	TCP/UDP 1813 (default) authentication port value + 1	Accounting	port1: Inbound	radius-acct
	RADIUS	TCP 2083 (default) User modifiable	RADIUS over TLS (RadSec)	port1: Bi-directional	radius-radsec
	RADIUS	TCP 389	Winbind (MSCHAPv2 authentication)	port1: Outbound	N/A
Meraki MX Controller	RADIUS	TCP/UDP	Authentication	port1: Bi-directional	radius-auth

Device Integration	Pro- tocol	Port	Description	Direction	Allowac- cess Option
		1812 (default) User modifiable			
	RADIUS	TCP 2083 (default) User modifiable	RADIUS over TLS (RadSec)	port1: Bi- directional	radius- radsec
	RADIUS	TCP 389	Winbind (MSCHAPv2 authentication)	port1: Outbound	N/A
	RADIUS	UDP 1700	Change of Authorization (CoA) or Disconnect	port1: Outbound	N/A
	HTTPS	TCP 443	Cloud Management- REST API (api.meraki.com)	port1: Outbound	N/A
Microsoft InTune MDM	HTTPS	TCP 443	Cloud Management - REST API Graph.windows.net manage.microsoft.co m Graph.microsoft.com	port1: Outbound	N/A
Mist Wireless	RADIUS	TCP/UDP 1812 (default) User modifiable	Authentication	port1: Bi- directional	radius- auth
	RADIUS	TCP/UDP 1813 (default) authenticatio n port value + 1	Accounting	port1: Inbound	radius- acct
	RADIUS	TCP 2083 (default) User modifiable	RADIUS over TLS (RadSec)	port1: Bi- directional	radius- radsec
	RADIUS	TCP 389	Winbind (MSCHAPv2 authentication)	port1: Outbound	N/A

Device Integration	Pro- to- col	Port	Description	Direction	Allowac- cess Option
	RADIUS	UDP 3799	Change of Authorization (CoA) or Disconnect	port1: Outbound	N/A
	HTTPS	TCP 443	Cloud Management - REST API api.mist.com (Default) User modifiable	port1: Outbound	N/A
SSO (Third Party)	RADIUS	TCP/UDP 1812 (default) User modifiable	Authentication	port1: Bi-directional	radius-auth
	RADIUS	TCP/UDP 1813 (default) authentication port value + 1	Accounting	port1: Inbound	radius-acct
	Agent Server	TCP 4568	Persistent Agent Communication	port1: Bi-directional port2: Bi-directional	nac-agent
Palo Alto Networks (Syslog Management)	Syslog	UDP 514	Logging of events to external server (outbound)	port1: Bi-directional	syslog
VPN - Checkpoint VPN - Palo Alto Networks	Syslog	UDP 514	Logging of events to external server (outbound)	port1: Bi-directional	syslog
	Agent Server	TCP 4568	Persistent Agent Communication	port1: Bi-directional port2: Bi-directional	nac-agent

SNMP trap support

The following table lists the traps and SNMP version supported by FortiNAC and the minimum FortiNAC version required. If a device has trap support that is not listed in this chart, see related [KB article 189853](#) for

details to requesting FortiNAC support for the trap.

Vendor	Trap Name	OID	SNMP Version	Minimum Supported Code Version
MIB 2	linkUp	0.3	1	8.x
	linkDown	0.2	1	8.x
	linkUp	1.3.6.1.6.3.1.1.5.4	2	8.x
	linkDown	1.3.6.1.6.3.1.1.5.3	2	8.x
HP	MACNotification	1.6.1.3.6.1.4.1.11.2.14.11.5.1.66	1	8.x
	MACNotification	1.3.6.1.4.1.11.2.14.11.5.1.66.0.1	2, 3	8.1.7
Aerohive	MACNotification	33.6.1.3.6.1.4.1.4413.1.1.1	1	8.0.6
Aruba	MACNotification	1.3.6.1.4.1.47196.4.1.1.1.101	1	9.2.1, 9.1.5
Arista	ARISTA_MAC_NOTIFICATION_MOVE	1.3.6.1.4.1.30065.3.2.0.1	1, 2 & 3	8.8.10, 9.1.0
	ARISTA_MAC_NOTIFICATION_ADD	1.3.6.1.4.1.30065.3.2.0.2	1, 2 & 3	8.8.10, 9.1.0
	ARISTA_MAC_NOTIFICATION_DELETE	1.3.6.1.4.1.30065.3.2.0.3	1, 2 & 3	8.8.10, 9.1.0
Extreme	MacAdded	1.3.6.1.4.1.1916.1.16.6.0.1	2	8.x
	MacDeleted	1.3.6.1.4.1.1916.1.16.6.0.2	2	8.x
	MacMoved	1.3.6.1.4.1.1916.1.16.6.0.3	2	8.x
Cisco	MacNotification	1.6.1.3.6.1.4.1.9.9.215.2	1	8.x
	MacNotification	1.3.6.1.4.1.9.9.215.2.0.1	2, 3	8.2.1
	cmnMACMoveFromPortId	1.3.6.1.4.1.9.9.215.1.3.5	1	9.1.6, 9.2.3
	cmnMACMoveToPortId	1.3.6.1.4.1.9.9.215.1.3.6.0	1	9.1.6, 9.2.3
D-Link	swL2macNotifyInfo	<sysObjectID>.2.100.1.2.0.1	2	8.8.10, 9.1.4, 9.2.0
	swL2macNotifyInfo	<sysObjectID>.2.100.1.2.1.1	2	8.8.10, 9.1.4, 9.2.0
H3C	MacNotification	1.3.6.1.4.1.25506.2.87.1.3.0.1	2	8.x
	MacNotification2	1.6.1.3.6.1.4.1.25506.2.87.1.4	1	8.x
	MacNotification3	1.3.6.1.4.1.25506.2.87.1.4	2	8.x

Vendor	Trap Name	OID	SNMP Version	Minimum Supported Code Version
	hh3cMACInformationChangedTrapExt	1.3.6.1.4.1.25506.2.87.1.4.0.1		8.7.5
	hh3cMACInformationMovedTrap	1.3.6.1.4.1.25506.2.87.1.4.0.2		8.7.5
Juniper	MacNotification	1.6.1.3.6.1.4.1.2636.3.40.1.7.2	1	8.1.10
	MacNotification	1.3.6.1.4.1.2636.3.48.1.0.5	2, 3	8.3.2, 8.2.11
Brocade/ Ruckus	Trap	1.3.6.1.4.1.1991	1, 2	8.x
	MacNotification	1.3.6.1.4.1.1991.0.201	1, 2	8.3.7, 8.5
Huawei	MacNotification	1.6.1.3.6.1.4.1.2011.5.25.315.3	1	8.2.1
	MacNotification	1.3.6.1.4.1.2011.5.25.315.3	2, 3	8.2.1
Fortinet	Device Detection	1.3.6.1.4.1.12356.101.1.639	2	8.7.6, 8.8.2
Fortinet	MacNotification	1.3.6.1.4.1.12356.106.2.0.706	1	9.2.6, 9.4.1
Dell	MacNotification	1.3.6.1.4.1.674.10895.5000.2.6132.1.1.1.0.34	1	F 7.2.0, 9.2.6, 9.4.1
NEC	necMACInformationMibTrapExt	1.6.1.3.6.1.4.1.119.2.3.126.10.2.87.1.4	1	F 7.2.2, 9.2.8, 9.4.3

SSH Algorithm Support

The following table lists the SSH authentication algorithms used by FortiNAC to establish SSH communications with network devices modeled in **Network > Inventory**.

The table below lists the algorithms enabled by default. It is possible to enable older algorithms, if necessary, to support older network devices. For instructions, see article [244991](#).

The supported list can also be found via CLI. See article [372269](#) (FortiNAC-OS).

Ciphers
3des-cbc
aes128-cbc
aes128-ctr
aes128-gcm@openssh.com
aes192-cbc
aes192-ctr
aes256-cbc
aes256-ctr
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com

Kex
diffie-hellman-group1-sha1
diffie-hellman-group14-sha1
diffie-hellman-group14-sha256
diffie-hellman-group15-sha512
diffie-hellman-group16-sha512
diffie-hellman-group17-sha512

Kex
diffie-hellman-group18-sha512
diffie-hellman-group-exchange-sha1
diffie-hellman-group-exchange-sha256
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
curve25519-sha256
curve25519-sha256@libssh.org
curve448-sha512

MAC
hmac-sha1
hmac-sha1-etm@openssh.com
hmac-sha2-256
hmac-sha2-256-etm@openssh.com
hmac-sha2-512
hmac-sha2-512-etm@openssh.com

Wireless security

In an environment that is predominantly wireless, where employees and guests are increasingly bringing personal devices and attempting to connect to the wireless network, wireless security is a powerful configuration tool. It allows you to quickly connect to wireless controllers and access points and configure the integration between those devices and FortiNAC.

Wireless devices are added to the **Network Devices** view based on their IP addresses. FortiNAC reads the configuration on the device. For any given wireless device you can configure multiple secure SSIDs (802.1x) or open SSIDs (unsecured) as needed. FortiNAC saves the SSID configuration to its own database.

Wireless security is currently only supported for Xirrus Arrays, HP MSM controllers, and Ruckus controllers. Other wireless devices can be added using the network devices View. See [Network devices on page 1](#).

For HP wireless devices in teaming mode, only the controller that is the team manager needs to be configured. Only the virtual IP address of the team should be used for configuration.

If you have purchased only the wireless only license and not the entire FortiNAC product, you can add only five wired devices. You cannot use discovery to scan the network for devices.

Implementation

General

1. Configure your wireless devices via the Admin Interface for each device. Make sure that hosts can connect to the network before integrating the devices with FortiNAC.
2. Review the integration document for your wireless device that is available on the Fortinet web site.
3. Use the Discovery option to enter IP address ranges and device credentials and search your network for devices. This option is not available if you have the Wireless Only License. See [Discovery on page 311](#).
4. Review the results of the Discovery process to make sure all devices have been found. If there are missing devices, check the IP address ranges entered, add any missing ranges and run the Discovery process again. See [Discovery results on page 313](#).
5. If you plan to authenticate network users through a directory, configure the integration with one or more directories. See [Directories on page 868](#).
6. Configure the Captive Portal. See [Portal configuration on page 631](#).

Guest Management

1. Configure guest templates. Guest templates control parameters of guest accounts, such as account duration, password length, or times when the network can be accessed, as well as the SSIDs to which guests can connect. Create a guest template for each unique type of guest. For example, if you have guests who should only have access from 9 in the morning until 5 in the evening, create a template for them. If you have guests who should only be allowed to access a special VLAN or Access Group, create a template for them.
2. If you would like to delegate guest account creation and management to other employees, create sponsor administrative accounts for those users. A sponsor account allows the user to log into the FortiNAC admin UI and create accounts for guests, send account credentials to guests and respond to guest self registration requests. See [Add a guest manager profile on page 175](#).
3. Create guest accounts as needed for incoming guests. See [Guest or contractor accounts on page 1](#).
4. Guest Management SSIDs configured using Wireless Security require at least one Guest Management SSID configuration for each guest template that is in use. Guests may connect to your network in other ways. If there are guest templates for guests that will never connect via one of the SSIDs you are configuring, those Templates do not require an SSID configuration.

Guest templates are part of the filter that determines the Access Group or VLAN to which the guest is assigned. If a guest has a guest template but the template has not been associated with an SSID the guest will not be able to access the network using one of the SSIDs configured through Wireless Security. The Guest may need to access the network using another wireless connection or a wired connection. SSID options include a Secure (802.1x) SSID or an Open SSID. See [Network devices on page 1](#) and [SSID mappings on page 76](#).

- For the Secure SSID configuration you must have a primary RADIUS server. If you do not have one

configured you can add it when configuring the SSID.

- For the Open SSID configuration you must provide the RADIUS secret configured on the array.

Device Onboarding

1. Add Secure (802.1x) or open SSIDs configurations for Device Onboarding to quickly register new devices and users on your network. See [SSID mappings on page 76](#).
 - For the Secure SSID configuration you must have a primary RADIUS server. If you do not have one configured you can add it when configuring the SSID.
 - For the Open SSID configuration you must provide the RADIUS secret configured on the device.
2. If your configuration requires that a Supplicant be installed on a device for it to connect to a Secure SSID, do the following:
 - Configure an Open SSID for Device Onboarding that contains a supplicant configuration with the security configuration for a Secure SSID. See [Supplicant configurations on page 600](#).
 - Configure the Secure SSID to which hosts or devices should connect after the Supplicant is installed. See [Secure SSID for device onboarding on page 80](#).

Auto-configured data

To simplify the configuration process for the Wireless Security feature some required pieces of data are generated automatically. For example, if you configure an SSID for guest access, the underlying user/host profile and network access policy are created for you.

Data Type	Data	Notes
Containers	Container Names: Wireless Controllers Wireless APs	Containers are used within FortiNAC to group devices together. As wireless devices are added using either Discovery or by entering them manually on the Network Devices View they are also added to Topology.
Port Groups	Group Names: Name of the Open or Secure SSID	Groups are used to gather like items that require similar treatment. The groups created here are port groups and are used to map network access policies for the Secure and Open SSIDs. When you configure an SSID a port group is created based on the name of the SSID. Each SSID is placed in a separate port group. For example if you add a SSID with the name MegaTech Secure, then a port group with the same name is automatically created and contains the MegaTech Secure SSID.
Host Groups	Group Names: Name of the group from the directory	Directory groups are used to group users and their corresponding hosts. Group membership is used in User/Host profiles to determine which network access, endpoint compliance, or Supplicant Policies to apply.

Data Type	Data	Notes
Model Configuration	Model Configuration: Name of the device	When a device that provides network services is added to FortiNAC a model of that device's configuration is stored in the database. This model includes information such as CLI User Names, Passwords, communication protocol, RADIUS server information and Isolation and Production VLANs. For devices configured through Wireless Security, the following settings are entered: • RADIUS = Use Defaults • Network Access = Deny for Dead End, Registration and Quarantine. Authentication is set to Bypass.
SSID Configuration	SSID Configuration: Name of the SSID	Individual SSIDs can be configured separately instead of inheriting settings from the device's Model Configuration, such as settings for default Isolation and Production VLANs. Use Network Devices View to select a device and access the SSID Configuration. For devices configured through Wireless Security, the following settings are entered for all SSIDs regardless of whether they are open or secure: • RADIUS: primary and secondary RADIUS servers are selected if they were selected in the SSID Mappings. • Network Access = Enforce and the Isolation VLAN are set for Dead End, Registration and Quarantine. Authentication is set to Bypass and None for Network Access.
Polling	L2 and L3 Polling settings	Wireless devices are automatically added to the L2 and L3 Polling groups and polling is enabled for the device. The polling interval for L2 is every 10 minutes and L3 is set to every 30 minutes. Use Network Devices View, L2 Polling View or L3 Polling View to modify polling information.
Roles	Role Names: Name of guest template associated with guest.	Roles are added as attributes to users or hosts. Role mapping is accomplished by creating a user/host profile configured with the SSID port group as the connection location and the Who/What by Attribute field set to one of these role names. A network access policy maps this user/host profile to a network access configuration containing the User Group/VLAN where the host will be placed. • A role is created for each guest template. • User/host profile contains an SSID port group (Where) and a Role name matching a guest template (Who/What by Attribute). • There is a separate user/host profile for each guest template and SSID port group combination.

Data Type	Data	Notes
User/Host Profile		User/host profiles are created when a new SSID Mapping is added on the Network Devices view. Guest Management SSID Mappings: A User/Host profile is created for each SSID and guest template combination. Names of these User/Host profiles are based on the SSID name and the combination of data contained within the profile.
Network Access Configuration Network Access Policy		Network access configurations and network access policies are created when a new SSID Mapping is added using Wireless Security. Guest Management SSID Mappings: A network access configuration and network access policy are created for each SSID and guest template combination. Names are based on the SSID name and the combination of data the items contain.
Endpoint Compliance Configuration Endpoint Compliance Policy		Endpoint compliance policies and endpoint compliance configurations are created when a device onboarding SSID Mapping with a supplicant configuration is added on the Wireless Security View. Device Onboarding: An endpoint compliance policy and endpoint compliance configuration are created for each unique SSID, directory group, host operating system, and supplicant configuration combination.
Supplicant EasyConnect Policy		A Supplicant EasyConnect Policy is created when a Device Onboarding SSID Mapping with a supplicant configuration is added on the Wireless Security View view. Device Onboarding: A Supplicant EasyConnect Policy is created for each unique SSID, directory group, host operating system, and supplicant configuration combination.
Portal Policy		A Portal Policy is created if a portal other than the default portal is selected when adding an SSID Mapping on the Wireless Security View for either Guest Management or Device Onboarding. Portal Policy: A Portal Policy is created for each unique SSID, directory group, host operating system and Portal combination.
Quarantine VLAN Switching	Enable	If a guest template or administrator profile limits network access by time, quarantine VLAN switching must be enabled. This allows FortiNAC to mark Guests and administrators as "At Risk" for the GuestNoAccess admin scan during the times they are not allowed to access the network. If Login Availability is set to Always for Guests and Administrators, the quarantine VLAN switching option is not enabled. Access this setting under System > Settings > Control.

SSID mappings

For supported wireless devices in the FortiNAC database you can configure Secure (802.1x) and Open SSIDs. The configuration is saved to the FortiNAC database. When configuring SSIDs, FortiNAC reads the existing configuration from the access point.

Supported wireless devices include: HP MSM Controllers, Ruckus Controllers and Xirrus Arrays.

The two primary functions for SSIDs configured through Wireless Security are to provide guest access and to allow network users to register devices on the network (Device Onboarding). Each of these functions can use either a Secure or an Open SSID and any given SSID can be used for more than one type of access.

Guest access

When Guest Management is selected, the Open SSID configuration includes access and isolation User Groups/VLANs, guest templates and the RADIUS secret. Existing Open SSIDs are read from the device by FortiNAC and they are displayed here.

The Secure SSID configuration for guest access includes access and isolation User Groups/VLANs, guest templates and RADIUS server information. These SSIDs are typically used by people with an 802.1x supplicant already installed on their wireless devices. Existing Secure SSIDs are read from the device by FortiNAC and they are displayed here. If a supplicant is required, this type of SSID may not be the best option for guests because the supplicant would need to be supplied separately.

Add or configure a Wireless Network (SSID) Mapping for each guest template. Guest templates control the SSIDs to which guests or users can connect. A guest account is created using a guest template. That association with the guest template remains on the guest account and a guest can ONLY connect to this SSID if the template on the account matches the template on the SSID Mapping. The same SSID can have multiple configuration records with different guest templates. Multiple SSID Mappings can have the same guest template.

Device onboarding

When Device Onboarding is selected, the Open SSID Mapping can limit access to the SSID based on the operating system of the connecting device. If you are authenticating through LDAP, only users who are in the selected directory group with one of the approved operating systems can connect to this SSID. The Mapping also includes access and isolation User Groups/VLANs selected from the configuration on the device. The Open SSID can be leveraged to serve a supplicant configuration to the connecting host for one of your Secure SSIDs.

The Secure SSID Mapping for Device Onboarding can limit access to the SSID based on the operating system of the connecting host. If you are authenticating through LDAP, the selected directory group also serves as criteria for connecting to this SSID. The Mapping includes RADIUS server information and access and isolation User Groups/VLANs selected from the configuration on the wireless device.

Supplicant configuration

Add or configure one or more Open SSIDs to serve supplicant configurations for Secure SSIDs, if needed. The supplicant configuration must be served via an Open SSID because it is the only SSID to which an unknown

user can connect.



Titles of windows and field names may vary depending on the brand of the device being configured. For example, HP devices use VSC to represent the record for the SSID and its configuration details. Screen shots and Settings were done using a Xirrus Wireless Array.

Settings

Field	Definition
SSID Name	Network name of the SSID configuration that includes all of the settings for the SSID, such as User Group.
SSID	Broadcast SSID Name Typically this is read from the array..
Mapping Type	Indicates whether this SSID Mapping is for Guest Management or Device Onboarding.
Guest Template	Guest template associated with this SSID. Only guests whose accounts were created with this guest template can access the network via this SSID.
Access User Group	Name or number of the network access identifier where a known host or device will be placed, such as User Group, VLAN ID or VLAN Name.
Isolation User Group	Name or number of the network access identifier, such as User Group, VLAN ID or VLAN Name, for the Isolation VLAN where an unknown host or device will be placed.
Operating Systems	Allows or denies access to an SSID based on the operating system of the connecting host. Options include: • Windows • macOS • iOS • Android • RIM • Windows Mobile
Directory Group	Allows or denies access to an SSID based on the directory group of the connecting user. If you are authenticating through RADIUS instead of LDAP, this option is hidden.
Supplicant Configuration	Name of the supplicant configuration that will be served to hosts that connect to the selected SSID. Only Open SSIDs used for Device Onboarding can serve supplicant configurations.
Portal Configuration	Name of the Portal that will be applied to hosts connecting via this SSID.
Primary RADIUS Server	RADIUS server that will be used by FortiNAC for authentication.
Secondary RADIUS Server	Secondary RADIUS server that will be used by FortiNAC for authentication if the primary RADIUS server cannot be reached.

Field	Definition
RADIUS Secret	Encryption key used by the RADIUS server to send authentication information. The RADIUS secret must be the same in FortiNAC RADIUS settings, on the SSID configuration and on the access point itself.
Buttons	
Apply To	Copies SSID Mappings to selected device models in the database based on matching SSID Names. Configure SSIDs in an environment where roaming is used and SSIDs must have the same configuration across multiple access points.

Secure SSID for guest management

1. Go to **Policy > Policy Configuration > Supplicant EasyConnect > Configuration**.
2. Click **System > Quick Start**.
3. Select **Network Settings > Network Devices** from the steps on the left.
4. Select a device in the Network Devices window.
5. Click **Wireless Security**.
6. On the SSID Mappings dialog, click **Add**.
7. Click the drop-down arrow in the **SSID Name** field and select the Name of the SSID to be mapped. These names are read from the wireless device and represent existing SSID configurations on the device.
8. Select **Guest Management**.
9. In the **Primary RADIUS** field select the RADIUS server that FortiNAC should use for authentication. If no RADIUS servers are configured, click **New** to add one. See [Legacy Proxy on page 381](#).
10. In the **Secondary RADIUS** field select the RADIUS server to be used in the event that the primary RADIUS cannot be accessed. This field is optional.
11. In the **Guest Template** field select the template that is required for guest access using this SSID.
12. In the **Portal Configuration** field select the captive portal that should be presented to the user when the host connects to this SSID. If you are not using multiple portals or you do not have a specific portal for this group of guests, select **Use Default**.
13. In the **Access User Group** field select the production User Group to be used for hosts accessing the Secure SSID using a guest account. These are read from the wireless device and represent existing User Groups that have been configured on the wireless device.
14. In the **Isolation User Group** field select the User Group to be used to isolate unknown hosts. These User Groups are read from the wireless device and represent existing User Groups that have been configured on the wireless device.
15. Click **OK** to save the SSID configuration.

Settings

Field	Description
SSID Name	Network name of the SSID configuration that includes all of the settings for the SSID, such as encryption method or VLANs.
Mapping Type	Device Onboarding: Indicates that this SSID Mapping will be used by known network users to register devices. Guest Management: Indicates that this SSID Mapping will be used by guests to access the network via a guest account.
Primary RADIUS Server	RADIUS server that will be used by FortiNAC for authentication.
Secondary RADIUS Server	Secondary RADIUS server that will be used by FortiNAC for authentication if the primary RADIUS server cannot be reached.
Guest Template	Guest template that must be associated with a guest account in order for the guest to connect on this SSID.
Portal Configuration	Name of the Portal that will be applied to hosts connecting via this SSID.
Access User Group	Name or number of the network access identifier where a known host or device will be placed, such as User Group, VLAN ID or VLAN Name.
Isolation User Group	Name or number of the network access identifier, such as User Group, VLAN ID or VLAN Name, for the Isolation VLAN where an unknown host or device will be placed.

Open SSID for guest management

1. Click **System > Quick Start**.
2. Select **Network Settings > Network Devices** from the steps on the left.
3. Select a device in the Network Devices window.
4. Click **Wireless Security**.
5. On the SSID Mappings dialog, click **Add**.
6. Click the drop-down arrow in the **SSID Name** field and select the Name of the SSID configuration to be added to the FortiNAC database. These names are read from the wireless device and represent existing SSID configurations.
7. Click **Guest Management**.
8. Click **Modify** next to the RADIUS Secret field. Enter the secret that is configured on the device.
9. In the **Guest Template** field, select the template that is required for guest access using this SSID.
10. In the **Portal Configuration** field, select the captive portal that should be presented to the user when the host connects to this SSID. If you are not using multiple portals or you do not have a specific portal for this group of guests, select **Use Default**.
11. In the **Access User Group** field select the production User Group to be used for hosts accessing the Secure SSID. These are read from the wireless device and represent existing User Groups that have been configured on the wireless device.

12. In the **Isolation User Group** field select the User Group to be used to isolate unknown hosts. These User Groups are read from the wireless device and represent existing User Groups that have been configured on the wireless device.
13. Click **OK** to save the SSID configuration.

Settings

Field	Definition
SSID Name	Network name of the SSID configuration that includes all of the settings for the SSID, such as encryption method or VLANs.
Mapping Type	Device Onboarding: Indicates that this SSID Mapping will be used by known network users to register devices. Guest Management: Indicates that this SSID Mapping will be used by guests to access the network via a guest account.
Guest Template	Guest template that must be associated with a guest account in order for the guest to connect on this SSID.
RADIUS Secret	Encryption key used by the RADIUS server to send authentication information. The RADIUS secret must be the same in FortiNAC RADIUS settings, on the SSID configuration and on the device itself.
Access User Group	Name or number of the network access identifier where a known host or device will be placed, such as User Group, VLAN ID or VLAN Name.
Isolation User Group	Name or number of the network access identifier, such as User Group, VLAN ID or VLAN Name, for the Isolation VLAN where an unknown host or device will be placed.

Secure SSID for device onboarding

If this SSID requires a supplicant configuration on the connecting host, the supplicant configuration can be served to the host through an Open SSID. Add the supplicant configuration to one of your Open SSIDs.

1. Click **System > Quick Start**.
2. Select **Network Settings > Network Devices** from the steps on the left.
3. Select a device in the Network Devices window.
4. Click **Wireless Security** at the bottom.
5. On the SSID Mappings dialog, click **Add**.
6. Click the drop-down arrow in the **SSID Name** field and select the Name of the SSID to be mapped. These names are read from the wireless device and represent existing SSID configurations on the device.
7. Click **Device Onboarding**.
8. In the **Primary RADIUS** field select the RADIUS server that FortiNAC should use for authentication. If no RADIUS servers are configured, click **New** to add one. See [Legacy Proxy on page 381](#).
9. In the **Secondary RADIUS** field select the RADIUS server to be used in the event that the primary RADIUS cannot be accessed. This field is optional.

10. In the **Directory Group** field select a group. The connecting user must be a member of this directory group to access the SSID. If you are authenticating through RADIUS instead of LDAP, this option is hidden.
11. In the **Allowed Operating Systems** section select one or more operating systems. The connecting host must have one of these operating systems installed to connect to this SSID.
12. In the **Portal Configuration** field select the captive portal that should be presented to the user when the host connects to this SSID. If you are not using multiple portals or you do not have a specific portal for this group of guests, select **Use Default**.
13. In the **Access User Group** field select the production User Group to be used for hosts accessing the Secure SSID. These are read from the wireless device and represent existing User Groups that have been configured on the wireless device.
14. In the **Isolation User Group** field select the User Group to be used to isolate unknown hosts. These User Groups are read from the wireless device and represent existing User Groups that have been configured on the wireless device.
15. Click **OK** to save the SSID configuration.

Settings

Field	Description
SSID Name	Network name of the SSID configuration that includes all of the settings for the SSID, such as encryption method or VLANs.
Mapping Type	Device Onboarding: Indicates that this SSID Mapping will be used by known network users to register devices. Guest Management: Indicates that this SSID Mapping will be used by guests to access the network via a guest account.
Primary RADIUS Server	RADIUS server that will be used by FortiNAC for authentication.
Secondary RADIUS Server	Secondary RADIUS server that will be used by FortiNAC for authentication if the primary RADIUS server cannot be reached.
Directory Group	Connecting user must be a member of the selected directory group to access this SSID. If you are authenticating through RADIUS instead of LDAP, this option is hidden.
Allowed Operating Systems	Allows or denies access to an SSID based on the operating system of the connecting host. Options include: • Windows • macOS • iOS • Android • RIM • Windows Mobile
Portal Configuration	Name of the Portal that will be applied to hosts connecting via this SSID.
Access User Group	Name or number of the network access identifier where a known host or device will be placed, such as User Group, VLAN ID or VLAN Name.

Field	Description
Isolation User Group	Name or number of the network access identifier, such as User Group, VLAN ID or VLAN Name, for the Isolation VLAN where an unknown host or device will be placed.

Open SSID for device onboarding

If you have a secure SSID that requires a supplicant configuration on the connecting host, the supplicant configuration can be served to the host through an Open SSID. Add the supplicant configuration to one of your Open SSIDs.

1. Click **System > Quick Start**.
2. Select **Network Settings > Network Devices** from the steps on the left.
3. Select a device in the Network Devices window.
4. Click **Wireless Security**.
5. On the SSID Mappings dialog, click **Add**.
6. Click the drop-down arrow in the **SSID Name** field and select the Name of the SSID for which you are adding a configuration in the FortiNAC database. These names are read from the wireless device and represent existing SSIDs.
7. Select **Device Onboarding**.
8. Click **Modify** next to the **RADIUS Secret field** and enter the RADIUS Secret configured on the device.
9. In the **Directory Group** field select a group. The connecting user must be a member of this directory group to access the SSID. If you are authenticating through RADIUS instead of LDAP, this option is hidden.
10. In the **Allowed Operating Systems** section select one or more operating systems. The connecting host must have one of these operating systems installed to connect to this SSID.
11. In the **Portal Configuration** field, select the captive portal that should be presented to the user when the host connects to this SSID. If you are not using multiple portals or you do not have a specific portal for this group of guests, select **Use Default**.
12. In the **Access User Group** field select the production User Group to be used for hosts accessing the Secure SSID. These are read from the wireless device and represent existing User Groups that have been configured on the wireless device.
13. In the **Isolation User Group** field select the User Group to be used to isolate unknown hosts. These User Groups are read from the wireless device and represent existing User Groups that have been configured on the wireless device.



The **Supplicant Configuration** field is optional. If you select a supplicant configuration that configuration is installed on the connecting host, allowing the host to connect to a secure SSID. See the table below for settings and [Supplicant configurations on page 600](#) for additional information.

14. Select a supplicant configuration from the drop-down menu. You can use the icons next to the **Supplicant Configuration** field to add a new configuration, delete a configuration or modify the configuration shown in the drop-down menu. Note that if you modify this configuration, it is modified for all features that make use of it.

15. To add a supplicant configuration, click **Add** next to the **Supplicant Configuration** field.
16. In the **Name** field, enter a name for this supplicant configuration.
17. In the **SSID** field, select the SSID that requires that a Supplicant be installed and configured on the connecting host.
18. In the **Security** field select a type from the drop-down list. Options include: Open, WEP, WPA, WPA2, WEP Enterprise, WPA Enterprise, WPA2 Enterprise.
19. Click in the **Password** field to open the Password pop-up. This is the Pre-Shared Key. Enter the key twice to confirm that it is correct and click **OK**. The Password field does not display if Open, WPA2 Enterprise or WPA Enterprise is selected in the Security field.
20. Click in the **Cipher** field and select AES, NONE or TKIP.
21. In the **EAP Type** field PEAP is the only option. EAP type does not display when Open, WEP or WPA is selected in the Security field.
22. The **Validate Server Certificate** field applies only to Windows 7 and higher hosts:
 - If disabled, it disables the Validate Server Certificate setting on the host and any certificate will be accepted.
 - If enabled, the host validates the Certificate with the list of Trusted Root Certificate Authorities listed in the host's Certificate Manager. If the CA is not listed on the host, the user may have to connect to the secure SSID manually.
23. If you have enabled WEP Enterprise, WPA Enterprise or WPA2 Enterprise the **CA Certificate** field is displayed. Browse to the CA or Root Certificate from the CA that issued the SSL certificate used on your RADIUS server. Select the file and click Open.
24. The **CA Fingerprint** field is displayed and automatically populated after a CA or Root Certificate is uploaded and the supplicant configuration is saved.
25. The **Note** field is optional.
26. Click **OK** to save the supplicant configuration.
27. In the **Primary RADIUS** field select the RADIUS server that FortiNAC should use for authentication. If no RADIUS servers are configured, click **New** to add one. Only displays if a supplicant configuration has been selected.
28. In the **Secondary RADIUS** field select the RADIUS server to be used in the event that the Primary RADIUS cannot be accessed. This field is optional.
29. Click **OK** to save the SSID configuration.

Open SSID settings

Field	Description
SSID Name	Network name of the SSID configuration that includes all of the settings for the SSID, such as encryption method or VLANs.
Mapping Type	• Device Onboarding: Indicates that this SSID Mapping will be used by known network users to register devices. • Guest Management: Indicates that this SSID Mapping will be used by guests to access the network via a guest account.
RADIUS Secret	Encryption key used by the RADIUS server to send authentication information. The RADIUS secret must be the same in FortiNAC RADIUS settings, on the SSID configuration and on the device itself.

Field	Description
Directory Group	Connecting user must be a member of the selected directory group to access this SSID. If you are authenticating through RADIUS instead of LDAP, this option is hidden.
Allowed Operating Systems	Allows or denies access to an SSID based on the operating system of the connecting host. Options include: • Windows • macOS • iOS • Android • RIM • Windows Mobile
Portal Configuration	Name of the Portal that will be applied to hosts connecting via this SSID.
Access User Group	Name or number of the network access identifier where a known host or device will be placed, such as User Group, VLAN ID or VLAN Name.
Isolation User Group	Name or number of the network access identifier, such as User Group, VLAN ID or VLAN Name, for the Isolation VLAN where an unknown host or device will be placed.
Supplicant Configuration	Contains the configuration for the SSID, Security Settings and password if required. This is optional. See the table below and Supplicant configurations on page 600 .
Primary RADIUS Server	RADIUS server that will be used by FortiNAC for authentication. Only displays if a supplicant configuration has been selected.
Secondary RADIUS Server	Secondary RADIUS server that will be used by FortiNAC for authentication if the Primary RADIUS server cannot be reached.

Supplicant configuration settings

Field	Definition
Name	User defined name for the Configuration.
SSID	Name of the SSID being configured. This is not necessarily the SSID to which the host is connected. However, the agent will attempt to move the host to this SSID when the configuration is applied. A host can have supplicant configurations stored for multiple SSIDs.

Field	Definition
Security	Indicates the type of encryption that will be used for connections to this SSID. Options include: • Open • WEP (PSK) • WPA (PSK) • WPA2 (PSK) • WEP Enterprise (PEAP) • WPA Enterprise (PEAP) • WPA2 Enterprise (PEAP)  WPA Enterprise and WPA2 Enterprise are limited to PEAP-MSCHAPv2.
Password	Opens the Password pop-up. This is the pre-shared key. Enter the key twice to confirm that it is correct and click OK. The Password field does not display if open, WPA2 enterprise, or WPA enterprise is selected in the Security field. The XML predefined characters ' " < > & are not supported.
Cipher	Encryption/decryption method used in conjunction with the information in the Security field to secure this connection. Options include: • AES • NONE • TKIP
EAP Type	Currently only PEAP is supported.
Validate Server Certificate	Applies only to Windows 7 and higher hosts. Default = Disabled. If disabled, it disables the Validate Server Certificate setting on the host and any certificate will be accepted. If enabled, the host validates the Certificate with the list of Trusted Root Certificate Authorities listed in the host's Certificate Manager. If the CA is not listed on the host, the user may have to connect to the secure SSID manually.
CA Fingerprint	Fingerprint parsed from the CA or Root Certificate from the CA that issued the SSL certificate used to secure the RADIUS server. This field does not display until after the certificate has been uploaded and the supplicant configuration has been saved.
CA Certificate	This field is only displayed if you select WEP Enterprise, WPA Enterprise or WPA2 Enterprise in the Security field. Select Choose File to browse to and select the CA or Root certificate from the CA that issued the SSL certificate used to secure the RADIUS server. CA or Root certificates can be downloaded from the CA web site. Either PEM or binary format can be used.
Note	User specified note field.

Dashboard

Terminology

The following terminology is used throughout this document and is defined here to avoid confusion.

- **Legacy View** - A view that is only available if the Legacy View Architecture flag is enabled. A Legacy View is one that has been rewritten in the new UI and displays in that form by default.
- **Legacy Dashboard** - This refers to the Dashboard available in FortiNAC through 9.1 as a Legacy View.
- **Dashboard** - Refers to the redesigned Dashboard built for 9.2.
- **Widget** - Formerly called Panel in our documentation, this term is used instead to align with the FortiGate.
- **Visualization** - A replacement for the tabbed view that the Legacy Dashboard had, a Widget has a selected Visualization which defines how it should render. Examples include "Pie Chart," "Table," and "Top Hosts." The set of available Visualizations differs per Widget.

Overview

The FortiNAC dashboard plays an essential role in gaining visibility upon all the devices connected to your network. Because some IT professionals may have very large numbers of devices, the dashboard is essential for gaining a "lay of the land" view of all network activity. You can choose which widgets are displayed and rearrange their order.

Upon booting up FortiNAC for the first time, you will see an empty dashboard. A fully running FortiNAC dashboard will look like this:

The screenshot displays the FortiNAC Dashboard interface. On the left is a navigation menu with options: Dashboard (selected), Main, Users & Hosts, Network, Policy & Objects, Portal, Logs, and System. The main content area features a '+ Add Widget' button at the top. Below it, the 'Endpoint Fingerprints' widget is active, showing a table of device information. The table has columns for Physical Address, Device Type, Operating System, IP Address, and Host Name. It lists several Apple iOS devices, including iPhone 6 Plus and iPhone 5S (GSM). At the bottom of this widget, it shows '8% 213 | Updated: 12:08:14'. Below the Endpoint Fingerprints widget is the 'Host Summary' widget, which provides a breakdown of host status. It includes a table with columns: Type, Total, Online Enabled, Offline Enabled, Online Disabled, and Offline Disabled. The data shows 214 Registered Hosts and 214 Safe&Authenticated hosts, with 1 online enabled, 213 offline enabled, 0 online disabled, and 0 offline disabled.

Physical Address	Device Type	Operating System	IP Address	Host Name
E0:B5:2D:38:2C:78	Apple iOS	iPhone 6 Plus		jtip52
E0:B5:2D:2C:F2:70	Apple iOS	iPhone 6 Plus		Chuo's i6+
DC:9B:9C:3B:95:9E	Apple iOS	iPhone 5S (GSM)		Lee's iPhone
D8:CF:9C:DB:A1:4A	Apple iOS	iPhone 5S (GSM)		Update 1-39
D8:CF:9C:DA:1A:E0	Apple iOS	iPhone 5S (GSM)		kPhone
D8:CF:9C:C4:78:94	Apple iOS	iPhone 5S (GSM)		Jason Bahls's iPhone
D4:F4:6F:41:A2:20	Apple iOS	iPhone 6		Blonde Phone

Type	Total	Online Enabled	Offline Enabled	Online Disabled	Offline Disabled
Registered Hosts	214	1	213	0	0
Safe&Authenticated	214	1	213	0	0

This section will cover details about the dashboard.

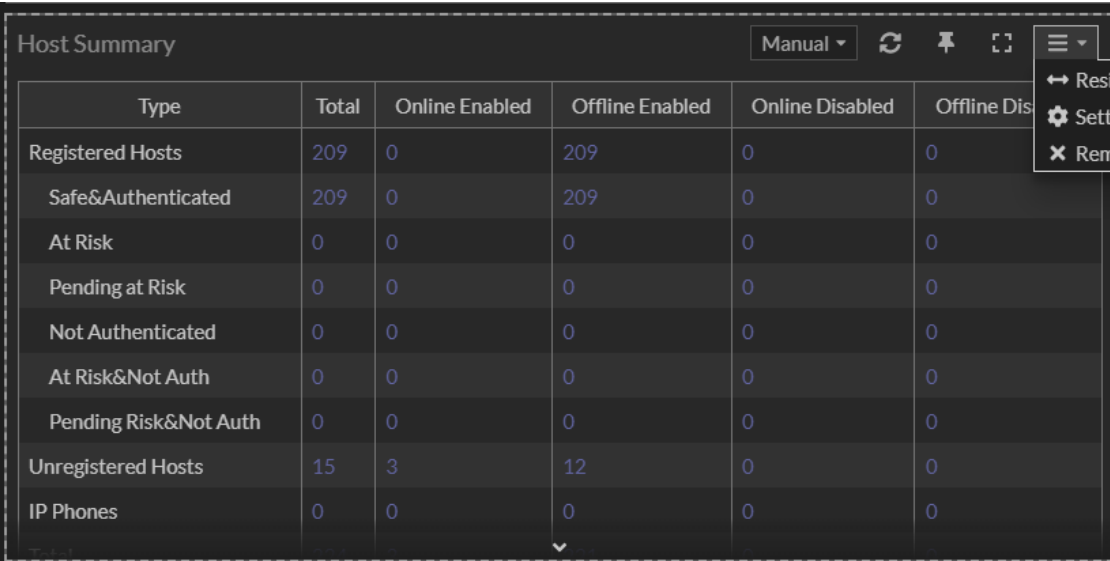
Note: FortiNAC saves dashboard preferences for each administrator, so one administrator's view on the same FortiNAC appliance may look different from another's without conflict. If the administrator has no defined dashboards, a dashboard is created with the name **Main** by default for all users, but this name may be changed.

Adding widgets

1. Go to any **Dashboard**.
2. Click **Add Widget**.
3. Select a widget from the list. When you select a widget, the settings for that widget are shown, if available for that type of widget. From the widget settings, if you would like to select a different widget, press Cancel to return to the list of widgets. You may add additional instances of widgets which already exist in the dashboard.
4. Click **OK**.

Widget Organization

The right hand corner of the widget contains a widget menu that contains options to resize, modify settings, and remove the widget.



Type	Total	Online Enabled	Offline Enabled	Online Disabled	Offline Dis
Registered Hosts	209	0	209	0	0
Safe&Authenticated	209	0	209	0	0
At Risk	0	0	0	0	0
Pending at Risk	0	0	0	0	0
Not Authenticated	0	0	0	0	0
At Risk&Not Auth	0	0	0	0	0
Pending Risk&Not Auth	0	0	0	0	0
Unregistered Hosts	15	3	12	0	0
IP Phones	0	0	0	0	0

All Widgets have a fixed height, but users can adjust the width set to the number of columns they should span.

Type	Total	Online Enabled	Offline Enabled	Online Disabled	Offline Disabled
Registered Hosts	209	0	209		
Safe&Authenticated	209	0	209		
At Risk	0	0	0		
Pending at Risk	0	0	0		
Not Authenticated	0	0	0		
At Risk&Not Auth	0	0	0		
Pending Risk&Not Auth	0	0	0		
Unregistered Hosts	15	3	12		
IP Phones	0	0	0		

Alarms

The Alarms widget has three different visualizations: **Table**, **Summary**, and **Graph** that can be swapped in the widget settings. FortiNAC can display alarm information from up to 60 days, available in Summary and Graph visualizations. The user has the ability to Acknowledge an alarm, thus marking for their own memory that they have seen this alarm. Control this function under Alarms settings.

Table

The Table visualization shows information about recent alarms, including when they occurred, what type of alarm, and the element affected. When you select an alarm from the list, you can perform the following actions:

- **Details:** View more details about the alarm, including the cause
- **Acknowledge:** Mark the alarm as acknowledged and sets the Time Acknowledged
- **Delete:** Deletes the alarm from the list

You can filter the list of alarms using the Filter button, displayed at the right side of each column header when you hover with your mouse.

Summary

Customize the time frame of this visualization under Alarm Settings > Previous Graph/Summary Days. The max archive age is 60 days. "For more information on the Archive Age Time setting, see [Database archive on page 977](#).

Graph

Customize the time frame of this visualization under **Alarm Settings > Previous Graph/Summary Days**. The max archive age is 60 days.

Endpoint Fingerprints

For information on Endpoint Fingerprints, see [Endpoint Fingerprints](#).

This widget displays either a list of, or summary of information regarding, Endpoint Fingerprints collected by FortiNAC.

This widget has three visualizations: **Table View**, **Top Operating Systems**, and **Top Vendors**. Table View is only available if the current user has Host permissions.

Table View

The Table View visualization is a limited version of the Endpoint Fingerprints view. Charts are not shown in this widget, in order to save space within the view.

Top Operating Systems

A summary of the Endpoint Fingerprints grouped by Operating System. The count of each slice is the total number of fingerprints which match that operating system.

Top Vendors

A summary of the Endpoint Fingerprints grouped by vendor. The count of each slice is the total number of fingerprints with a physical address matching each vendor.



Rogue record is created and populated with the information collected from the various endpoint fingerprint sources. The device is only automatically registered if it matches a Device Profiling rule that is configured to automatically register. Otherwise, it remains a Rogue.

If the Vendor OUI is not yet recognized, FortiNAC will not be able to register the device. See [Vendor OUIs](#).

Set Source Rank

The order used when processing fingerprint sources for populating an endpoint's host record, starting at rank 1.

Example:

1. Agent—processes info from endpoint's agent first and populates host record
2. DHCPv4—processes info collected from endpoint's DHCP packets second and populates host record
3. Vendor OUI—processes endpoint's OUI info last and populates host record

Last Heard Time

The most recent time FortiNAC received information from that specific method. Example: The last time FortiNAC received a DHCP packet for the endpoint.

Host Summary

The Host Summary widget displays information about the hosts on your network. You can view the total number of each type of host, as well as information about whether hosts are online or offline, and if hosts are enabled or disabled.

Host Summary					
Manual ↻ 📌 🔍 ☰					
Type	Total	Online Enabled	Offline Enabled	Online Disabled	Offline Disabled
Registered Hosts	209	0	209	0	0
Safe&Authenticated	209	0	209	0	0
At Risk	0	0	0	0	0
Pending at Risk	0	0	0	0	0
Not Authenticated	0	0	0	0	0
At Risk&Not Auth	0	0	0	0	0
Pending Risk&Not Auth	0	0	0	0	0
Unregistered Hosts	19	3	16	0	0
IP Phones	0	0	0	0	0
Total	228	3	225	0	0

Registered hosts fall into one of six different states:

- **Safe & Authenticated:** Hosts that have not failed a scan and have an associated user that is authenticated.
- **At Risk:** Hosts that failed a scan or which are manually marked by the administrator as at risk.
- **Pending at Risk:** Hosts that failed a scan but have not been marked as at risk because of the delayed remediation settings in the endpoint compliance policy used. For more information, see [Delayed remediation on page 546](#).
- **Not Authenticated:** Hosts that have an associated user that is not authenticated.
- **At Risk & Not Authenticated:** Hosts that failed a scan or that an administrator has manually marked at risk and have an associated user that is not authenticated.
- **Pending Risk & Not Authenticated:** Hosts that failed a scan but have not been marked as at risk because of the delayed remediation settings and have an associated user that is not authenticated.

The panel also shows a count for hosts that are not registered, as well as a separate count for IP phones. Each state for the hosts is further divided into different statuses:

- **Total:** All hosts in this state, regardless of status.
- **Online Enabled:** The host is enabled and is currently on the managed network.
- **Offline Enabled:** The host is enabled, but is not currently found in the managed network.
- **Online Disabled:** The host is disabled and is currently on the managed network, including in isolation states.
- **Offline Disabled:** The host is disabled and is not currently found in the managed network.

This widget has two different visualizations that can be accessed through the widget settings or by expanding the widget: **Table View** and **Pie Chart**.

Table View

The Table View visualization displays each host state as a single row, including rows for All Registered Hosts and All Hosts. For each row, the different host statuses appear as a column. Clicking the number will navigate

to the Hosts view with an automatically applied filter to show hosts in that state and status.

Pie Chart

The Pie Chart visualization displays each host state as a slice. Hovering the slice provides a tooltip which divides the host state into each status. Clicking on the number will navigate to the Hosts view with an automatically applied filter to show hosts in that state and status.

User Summary

The User Summary widget displays information about the user and guests in FortiNAC.

Type	Total	Enabled	Disabled
User Registrations	5	5	0
Guest Registrations	0	0	0

This widget has two different visualizations that can be interchanged through the widget settings or simultaneously displayed when expanded: **Table View** and **Pie Chart**.

Table View

User and Guest Registrations are displayed based on their enabled state. Click on the number to navigate to the User Accounts view with an automatically applied filter to show the matching users.

Pie Chart

A summary of the total number of users and guests, both enabled and disabled, is displayed as a pie chart.

License Information

This widget displays information about the licenses for our device, including the total number of licenses, how many are currently in use, how many unused licenses are available, and entitlements.

Note: The License Expiration date listed is within days of the actual date. To confirm the exact date, login to the Fortinet Support Portal (<https://support.fortinet.com>).

Table View

The more complete view of license information, this visualization displays the number of available and used licenses, and all entitlements.

You can modify the thresholds used to determine when % Used displays as Warning or Critical. By default, the threshold for Warning is 75% and Critical is 95%. To modify the thresholds, click on the colored bar and enter the new thresholds. Threshold changes are global and affect all users. Changing these thresholds also influences when the associated Events will be generated.

For more information, see [Licenses on page 29](#).

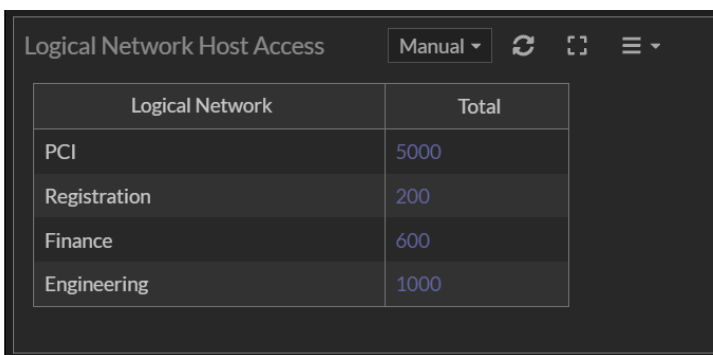
Pie Chart

A summary of the available and in use licenses are displayed as slices in a pie chart.

Logical network host access

This feature displays all Hosts that had access to each Logical Network over a configurable period of time. This feature is especially useful if the user knows which type of network activity they want to investigate; the user can then see all the hosts that were connected to a particular Logical Network for a specified time period.

Example



The screenshot shows a widget titled "Logical Network Host Access" with a "Manual" dropdown, a refresh icon, a full-screen icon, and a menu icon. Below the header is a table with two columns: "Logical Network" and "Total". The table contains four rows of data.

Logical Network	Total
PCI	5000
Registration	200
Finance	600
Engineering	1000

Monitors

Monitors are a special type of dashboard which displays a single widget in a maximized view. They are rendered in a separate group from other dashboards. **Note:** not all widgets have a monitor feature as of v7.2.0.

A default monitor gets created as part of the dashboards for any new Admin User that is added.

Add a monitor

1. Go to **Dashboard**.
2. Hover over the **Add Dashboard** button.
3. Click the **Actions** icon. The option to **Add Monitor** will appear.
4. Click **Add Monitor**.

Network Device Summary

The **Network Device Summary** widget displays information about the network devices and ports managed by FortiNAC.

Network Device Summary			
Manual   			
Device	Total	Operating	Error
Server	1	 1	 0
Wireless Access Point	3	 3	 0
Switch	2	 2	 0
Ports	283	 172	 111

This widget has three different visualizations: **Table View**, **Enforcement Chart**, and **Pie Chart**.

Pending Tasks

For details on creating and managing Tasks, see [Tasks](#).

Widget Capabilities

- Communicate with other system administrators to reduce workload on any single admin
- If you are the supervisor, provide daily tasks to other admins
- You can give other admins less privileges in **User & Hosts > Administrators**



Tasks may also be automatically created by the system, such as when running the Guided Install .

This widget displays a tree of tasks which either have been assigned to the currently logged in administrator or are assigned to everyone. This widget contains no settings.

Each record in the widget contains the same controls which appear in the menu in the header. Progress meters will appear within this widget, but will only update based upon the update interval settings of the widget.

Recent hosts

The Recent Hosts widget displays newly discovered hosts by type. This feature makes it easy for the user to get the count of every different type of new hosts. Clicking into the Count can zoom into a list of all hosts of a given type.

Note: The "new" host status is based on host creation date, as opposed to date via registration logs.

System Performance

This panel displays information about the current performance of your FortiNAC

It has two visualizations: **Table View** and **Chart**.

Table View

This visualization displays a detailed look into the total, free, and used percentage of the FortiNAC appliance's memory and partitions. You can modify the thresholds used to determine when % Used displays as Warning or Critical in both the Hardware and Software tabs. By default, the threshold for Warning is 85% and Critical is 95%. Threshold changes are global and affect all users. Changing these thresholds also influences when the associated Events will be generated.

Chart

The Graph visualization monitors the system's overall CPU and memory usage. A maximum number of data points, up to 100, may be configured in the settings as the "Maximum Graph Size." The oldest data points are removed from the graph when any are added in excess of this value.

Persistent Agent Summary

The **Persistent Agent Summary** panel displays information about hosts using the Persistent Agent.

This widget has two visualizations: **Table** and **Pie Chart**.

Table

This visualization lists hosts by agent version and by operating system. Only hosts using the Persistent Agent are counted in this panel. To view more information about the hosts, click the number in the **Total** or **Operating System** column.

Pie Chart

A summary of the persistent agents, each slice in the pie chart represents a combination of OS and agent version.

RADIUS Activity

Displays information from **Network > RADIUS**.

Current – Displays the latest success/failure information.

Displays a donut chart showing the number of authentication successes vs authentication failures over a specified timeframe (1 hour default). This can be configured to show success and failure only, or success and each detected failure cause. **Note:** All pie pieces beside the Access-Accept slice can be selected, and will open the secondary RADIUS – Rejected Hosts view giving a view of the specific requests that contributed to that failure cause.

Timeline – Displays success/failure information over time.

Displays a stacked area showing the same information over time. This can be configured to show success & failure only, or success and each detected failure cause.

Historical Comparison – Compares timespans of success/failure information

Displays a table which compares the latest success/failure information with the same timespan the previous hour, day, and week, as well as against the average for that timespan for all past same day of the week. For example, if the view is showing the past hour of activity, and it's Tuesday at 9am, then the table would show comparison results against 8am that morning, the previous Monday at 9am, Tuesday at 9am from the previous week, and the average activity for all previous Tuesdays at 9am. This is intended to help expose any significant drops in RADIUS activity that could be occurring because of a loss of connectivity to devices in the network that are no longer able to reach FortiNAC to authenticate users.

Security Summary

This widget displays information about incoming security events and related alarms, and has the following visualizations: **Summary**, **Top Alarms**, **Top Hosts**, and **Top Events**. Every visualization contains an adjustable time period across which they will be summarized.

Widget capabilities

- Go to its settings to toggle its views
- Get at-a-glance information of alarms, hosts, and events - sorted in importance and frequency.

Scans

The Scans widget displays information about recent scans.



This widget may display different data than Scan Results, because information in the panel is retrieved from a different database. The Scans panel is also not affected by the scheduled archive and purge of scans. For more information, see [Scan results on page 804](#).

This widget features three different data groups: **By Day**, **By Hour**, and **Overall**. When selecting By Day or By Hour, a visualization of either **Line Chart** or **Stacked Area Chart** is available. Available from the settings is a default set of filters to use for the data, but these filters may be changed from their default value in the widget.

Note: Changing the values from their default is not saved and will be lost when navigating away from the dashboard.

By Day

Scan results are grouped by result per day over the supplied time period. This may be displayed either as a line chart or a stacked area chart. The date range may not exceed 90 days for this data grouping.

By Hour

Scan results are grouped by result per hour over the supplied time period. This may be displayed either as a line chart or a stacked area chart. The date range may not exceed 3 days for this data grouping.

System Summary

The System Summary widget displays information about the FortiNAC cluster. This widget contains no settings. A cluster may contain up to 4 FortiNAC appliance by having a High Availability configuration with both Control and Application servers.

Status displays the current status of each FortiNAC appliance:

- **Running:** The FortiNAC is running.
- **Not Reachable:** The dashboard cannot communicate with the FortiNAC.
- **Management Down:** The FortiNAC is running but the software is down.
- **Running - Idle:** The FortiNAC is running but there is currently no activity.
- **Running - In Control:** The FortiNAC is running and is in control in a high availability environment.
- **Running - Not In Control:** The FortiNAC is running and is not in control in a high availability environment.

To restart the primary server and resynchronize data in a high availability environment, click **Resume Control**. This option is available only when the secondary server is in control. For more information, see [High availability on page 1](#).

Top host activity

This feature displays the hosts with the most connection activity over a configurable period of time. The default time range is 7 days.

Top Host Activity			
Device Type	Total Connections	Host Name	Username
Windows	5	JoeLaptop	Joe Doe
Printer	2	BRW9CAD9 765FB7B	
Apple iOS	3		
Camera	5		

Menus

The main menu is located along the left side of the window at all times and includes the following expandable options: Dashboard, Users & Hosts, Network, Policy & Objects, Portal, Logs, and System

Changing the theme

You can change the admin UI theme by clicking the User icon in the top right corner. Select **Preferences** > use the **Theme** field.

FortiNAC saves preferences for each individual user.

Favorite menu tabs

It is possible to favorite menu tabs with a gold star. They will then appear at the top of the menu, under Favorite.

Dashboard

Dashboard Menu	Topic
Multi-Dashboard Feature	Dashboard on page 86

Users & Hosts

Users & Hosts menu	Topic
Administrators	Administrators on page 119
Admin Profiles	Administrator profile on page 174
Guests & Contractors	Guest or contractor accounts on page 1
Guest/Contractor Templates	Guest & Contractor templates on page 164
Account Requests	Sponsors can approve or deny account requests for accounts from guests using the self registration feature.
Registration Requests	Guest self registration on page 188
User Accounts	User accounts on page 194
Hosts	Hosts on page 213
Adapters	Adapter View on page 237
Applications	Application view on page 243
Endpoint Fingerprints	
Profiled Devices	Configure profiled devices on page 252
Device Profiling Rules	Device profiling rules on page 259
Network Sessions	Network sessions on page 274
Locate	Locate hosts on page 276
Manage Hosts & Ports	Manage hosts and ports on page 283
Send Message	Send messages to hosts on page 288
Settings	Settings on page 863

Network

Network menu	Topic
Inventory	Inventory on page 289
Logical Networks	Logical networks on page 373
RADIUS Settings	RADIUS on page 375
Service Connectors	Configure one or more Mobile Device Management (MDM) servers that integrate with FortiNAC. See MDM Servers on page 413 .
CLI Configuration	CLI configuration on page 433
L2 Polling	L2 polling on page 449
L3 Polling	L3 polling on page 451

Network menu	Topic
Connections	Connections view on page 1
Port Changes	Port changes on page 455
Settings	Settings on page 863

Policy & Objects

Policy menu	Topic
User/Host Profiles	User/host profiles on page 466
Portal Policy	Portal policy on page 471
Authentication	Authentication on page 475
Network Access	Network access on page 482
Endpoint Compliance	Policies on page 531
Supplicant EasyConnect	Supplicant EasyConnect on page 595
Passive Agent	Passive Agent on page 604
Remediation Configuration	Remediation configurations on page 615
Roles	Roles on page 620
Network Device Roles	Roles on page 620

Portal

Portal Menu	Topic
Portal Configuration	Portal configuration on page 631
Request Processing Rules	Request Processing Rules on page 741
Portal SSL	Portal SSL on page 745

Logs

Logs menu	Topic
Audit Logs	Audit Logs on page 746
Events & Alarms	
Alarms	Alarms on page 783
Events	Events on page 749
Mappings	Map events to alarms on page 784
Management	Event management on page 772

Logs menu	Topic
Reports	Reports on page 793
Scan Results	Scan results on page 804
Security Incidents	
Events	Events on page 814 Only available when Security Incidents is enabled within your current license package.
Alarms	Alarms on page 815 Only available when Security Incidents is enabled within your current license package.

System

System menu	Topic
Certificate Management	Certificate management on page 828
Config Wizard	Guided Install on page 28
Groups	Groups on page 843
Feature Visibility	Feature Visibility on page 856
Scheduler	Scheduler on page 857
Tasks	Tasks on page 862
Settings	Settings on page 863

Feature Visibility

System > Feature Visibility provides the ability to enable or disable structural visibility changes to the FortiNAC style.

Option	Description
Unified Settings	Compress all four Settings views into a single Settings view under the System category
Legacy View Architecture	Switches views which have been upgraded back to the older FortiNAC style. Note: Legacy View Architecture is no longer supported in v7.6

Import and export data

Importing and exporting data allows you to leverage information across products, manipulate data outside your software or restore archived data. Import and export methods vary greatly depending on the type and location of the data. Review the tables below for information on import and export types and links to corresponding instructions.

Import types

Type	Definition
Import archived data on page 102	FortiNAC periodically archives and purges data from the database. Use this import to retrieve archived data for review.
Import hosts, users or devices on page 102	Allows you to import hosts, users with associated hardware, devices and IP Phones.
Import an administrator on page 109	Allows you to import data for administrators.
CLI import tool on page 112	A command line tool that allows you to import lists of devices by type into a selected container in the Inventory.
Import port descriptions on page 116	Allows you to import port descriptions into the Inventory from a .csv file.
Import IP ranges on page 112	Allows you to import ranges of IP addresses into the access point management configuration view.
Import portal content	Allows you to import previously exported portal pages.
Bulk guest import on page 159	Allows you to import guest data from a text file to be used when creating bulk accounts.

Export types

Type	Definitions
Export data on page 116	Allows you to export data from table views in FortiNAC.
Add a custom report on page 798	After generating a custom report, you can export the data it contains.
Add Conference Accounts on page 160	Guest/contractor account views that allow you to export the data displayed.
Add Bulk Accounts on page 158	
Add Single Account on page 156	
Export portal content on page 647	Allows you to export portal pages configured with the portal configuration content editor.

Type	Definitions
License Information on page 92	Allows you to export data from the License Usage dialog. Click on the number in the In Use column on the License Information panel to open License Usage dialog. Export options are displayed at the bottom of the window.

Import archived data

When the Purge Events task runs, FortiNAC creates an archive of several different types of records. You can reimport this data if necessary. Importing archived data does not overwrite existing data it adds the archived records back into the database. Records that are archived and can be re-imported include the following:

- [Alarms on page 783](#)
- [Events on page 749](#)

1. Navigate to one of the views listed above.
2. Click **Import**.
3. Select the **archive** from the drop-down list. The archives are listed by date with the name of the view at the beginning. For example, for the Connections View the archive would have the following format:
DYNAMICLOG_Archive_YY_MM_DD.bua.gz
4. Click **OK**.

Some archive files can be quite large and make take several minutes to import. A progress dialog is displayed as the import is taking place. A message is displayed when the import is complete.

Import hosts, users or devices

Hosts, users or devices can be imported into the database from a .csv (comma separated value) file. Devices imported through the Host View are displayed in the Host View.

Create an import file

To add Hosts, users, devices or IP Phones create a comma separated value (.csv) file using any text editor or spreadsheet tool. If you are using a text editor to create the file, use commas to separate the fields when you enter the data. Use carriage returns to separate records. You can mix the types of records you are importing. For example, you can import hosts, users and IP Phones in the same file as long as you have all of the appropriate fields in the header row.

To add Hosts or Devices create a comma separated value (.csv) file using any text editor or spreadsheet tool. If you are using a text editor to create the file, use commas to separate the fields when you enter the data. Use carriage returns to separate records.

The first row in the file is a header row and must contain a comma separated list of the database field names that are included in the import file. The order of the fields does not matter. For example, to import hosts and their corresponding adapters the header row could have the following fields:

```
adap.mac, adap.ip, host.owner, host.host, siblings
```

Unless otherwise specified, data type is a string with no size limitations. Fields are case sensitive. For example, if you have user IDs SMITH123 and Smith123, the database treats these as two separate user records.

If you import something that already exists in the database, the existing record is updated with the new data from the import. For example, assume the database contains a host record with MAC address A0:11:22:BE:44:2C, IP address 192.168.10.102 and host name Taylor1 and you import a record that has MAC address A0:11:22:BE:44:2C, IP address 192.168.5.10 and host name Jones1. The MAC address remains the same since that is the key, but the other fields are updated. The database now contains a host record with MAC address A0:11:22:BE:44:2C, IP address 192.168.5.10 and host name Jones1.

Imported data is displayed on multiple views. Adapter data is displayed on the **Adapter View** and in **Adapter Properties**. Host data is displayed in the Host View, in **Host Properties**. User data is displayed in the **User View** and **User Properties**.

The table below lists all of the possible import data fields by the name that should be used in the header row, indicates which fields are required and provides a definition for each field.

Fields

Header Field	Required For	Properties Field: Definition
Adapter		
adap.ip		IP address: IP address of the adapter. Use a valid IP format, such as 127.0.0.1.
adap.mac	host	Physical Address: MAC address of the adapter. Use a valid MAC format, such as 00:19:D1:94:5C:06.
adap.loc		Location: The switch and port where the adapter is connected to the network.
adap.media		Media Type: Network interface type (wired or wireless).
adap.accessVal		Access Value: VLAN to which the adapter is assigned.
adap.descr		Description: Description of the adapter, such as Intel(R) 82566DM Gigabit Network Connection.
adap.venName		Vendor Name: Name of the vendor for the adapter based on the first three octets of the MAC address, such as Intel Corporation. vendor OUIs are stored in the database and can be viewed through the vendor OUI screen. See Vendor OUIs on page 898 .
Host view		
host.host		Host Name: Name of the host.

Header Field	Required For	Properties Field: Definition
host.role		Role: Roles are attributes on hosts that can be used as filters by FortiNAC when selecting a network access policy, an endpoint compliance policy or a Supplicant EasyConnect Policy. The role must be defined in FortiNAC and must be the same spelling and case. If the role field is blank or is not included in the import the host is assigned to the NAC-Default role.
host.owner		Registered User: User ID of the host's owner. On import FortiNAC checks for the user in its own database and in the LDAP directory. If the user does not exist a new user record is created. If the user does exist the user is connected to the host.
host.expireDate		Expiration Date: Date that the host is aged out of the database. Date format is MM/dd/yy HH:mm AM/PM Timezone or 04/07/10 08:11 AM EST. If not included in the import, the global setting in FortiNAC Properties is used. See Aging on page 1006. The value "Never" can be used to prevent a host from ever being removed from the database by the aging process. Host age times are evaluated every ten minutes. If you specify a date and time, the host may not be removed from the database for up to ten minutes after the time selected.
host.inact		Days Inactive: the host can be inactive before being aged out. This number is used to calculate the date to age the host out of the database. If not included in the import, the global setting in FortiNAC Properties is used. See Aging on page 1006. To avoid using the default settings you must enter a number in this field. You can use a very large number to ensure that the host is not deleted, such as 1825 Days (equals five years). Make sure that there is a space between the number and the word Days. The format for the value must be as follows: xxx Days 1825 Days
host.sn		Serial Number: Serial number of the host.
host.hwType		Hardware Type
host.os		Operating System: Host's operating system such as Windows XP or macOS.  Only hosts that have an operating system listed in Host Properties are rescanned at the scheduled rescan time. Valid operating systems include: Windows or Mac.

Header Field	Required For	Properties Field: Definition
host.agentTag		Asset Tag: Arbitrary value assigned in the BIOS by the owner or manufacturer.
host.agentVer		Agent Version: Version number of the Persistent Agent installed on the host.
host.hasAgent		Persistent Agent: Indicates whether or not the host has an agent installed. Use true or false. If the field is left blank, the default is false.
host.notes		Notes: Data is imported into the Notes field in Host Properties.
host.topo	host - if importing into Inventory	Topology: Container in Inventory where this host should be placed on import. This field is required if importing into Inventory. Host is managed by the Host View but displays in both the Host View and the Inventory.
host.dirPolVal		Security And Access Value: Security and Access Value is an attribute used as a filter for user/host profiles. Typically this is a value that comes from the user record in the directory. However, if you are not authenticating through a directory or if this host does not have an owner, the Security and Access Value can be entered manually.
host.devType		Device Type: Must be one of the following device types or blank: • Alarm System • Android • Apple iOS • Camera • Card Reader • Cash Register • Dialup Server • Environmental Control • Gaming Device • Generic Monitoring System • Health Care Device • Hub • IP Phone • IPS / IDS • Linux • macOS • Mobile Device • Network • PBX • Pingable • Printer • Registered Host

Header Field	Required For	Properties Field: Definition
		• Server • StealthWatch • Top Layer IPS • Unix • UPS • Vending Machine • Windows • Wireless Access Point • VPN
siblings		Siblings: Adapters that are on the same host are siblings. For example, if a PC has a wireless adapter and a wired adapter, those adapters are siblings. Enter the MAC addresses of all of the adapters for this host separated by semi-colons (;). See the example below: 00:15:70:CA:7D:01;00:15:70:CA:7D:00 Each adapter must have a separate record in the .csv file, with a siblings field listing all of the adapters on the host. Some device types may have only one adapter, such as IP Phones. To import those devices, include the MAC address of the single adapter in the siblings field with no semi-colon.
User		
authType		Local: local user RADIUS: RADIUS user LDAP: LDAP user  If "authType" is set to "LDAP" the user record will sync with the directory
user.fn		User's first name.
user.ln		User's last name.
user.uid	user	ID: Unique alpha numeric user ID. If a directory is used for authentication, when the FortiNAC database is synchronized with the directory, data for users with matching IDs is overwritten with data from the directory. For example, if you import a user with ID AB118 named Ann Brown and the directory contains a record of AB118 as Andrew Bowman, then your database shows AB118 Andrew Bowman.
user.email		User's e-mail address. For multiple e-mail addresses, enter addresses separated by commas or semi-colons. Messages are sent to all e-mail addresses provided.

Header Field	Required For	Properties Field: Definition
user.addr		User's mailing address.
user.city		User's city.
user.st		User's state.
user.zip		User's postal code.
user.ph		User's telephone number.
user.title		User's title.
user.role		Role: Roles are attributes on users that can be used as filters by FortiNAC when selecting a network access policy, an endpoint compliance policy or a Supplicant EasyConnect Policy. The role must be defined in FortiNAC and must be the same spelling and case. If the role field is blank or is not included in the import the host is assigned to the NAC-Default role.
user.notes		Notes: Data is imported into the Notes field in User Properties.
user.pw		Password: Password for this user.
user.dirPolVal		Security And Access Value: Security and Access Value is an attribute of a user that can be used as a filter for user/host profiles. Typically this is a value that comes from the user record in the directory. However, if you are not authenticating through a directory the Security and Access Value can be entered manually.
user.expireDate		Expiration Date: Date that the user is aged out of the database. Date format is MM/dd/yy HH:mm AM/PM Timezone or 04/07/10 08:11 AM EST.
user.maxHosts		Allowed Hosts: Maximum number of hosts that can be associated with or registered to this user and connect to the network.
user.delHosts		Delete Associated Hosts: Indicates whether or not hosts registered to this user should be deleted when the user is aged out of the database. Enter either Yes or No . This data displays on the User Properties window in the Time section and is set when the expiration date is set. Importing this field requires that you also include user.expireDate in your import file. If you do not include user.expireDate , the user.delHosts field data is not imported.
user.smsNum		Mobile Number: User's mobile phone number. This can be used to send SMS Messages based on events and alarms.

Header Field	Required For	Properties Field: Definition
user.smsPro		Mobile Provider: The carrier or provider for the user's mobile phone. This must match the name of one of the providers in the Mobile Providers list in the database. See Mobile providers on page 1 .

Sample import files

Hosts, adapters, users, or devices can be imported through the hosts view using a .csv file. All of these items can be included in the same import file as long as the header row contains the appropriate database field names. Below are sample import files for each type as well as an import file containing records of all types.

Host import

The `adap.mac` field is required for this import.

```
adap.mac,siblings,adap.ip,host.owner,host.devType
00:13:CE:6C:56:75,00:13:CE:6C:56:75,192.168.20.45,Smith2010,Windows
00:15:70:D9:46:B0,00:15:70:D9:46:B0;00:15:70:D9:46:B1,,Orr2010,Linux
00:15:70:D9:46:B1,00:15:70:D9:46:B0;00:15:70:D9:46:B1,,Orr2010,Linux
```

Pingable device import

The `adap.mac` field is required for this import. The `host.devType` field is recommended to ensure that the correct icon displays. Use the `host.topo` field to display this device both in the Host View and Inventory. Entering the name of the Inventory container in the `host.topo` field triggers FortiNAC to display the device in the Inventory. The device is automatically displayed in the Host View.

```
adap.mac,siblings,adap.ip,host.topo,host.devType
00:13:CE:6C:56:75,00:13:CE:6C:56:75,192.168.20.45,Blding_B,PBX
00:15:70:D9:46:B0,00:15:70:D9:46:B0,192.168.20.10,Blding_A,Camera
00:15:70:D9:46:B2,00:15:70:D9:46:B2,192.168.20.12,Blding_A,Printer
```

IP phone import

The `adap.mac` field is required for this import. The `host.devType` field is not required; however, since IP phones are treated differently to prevent dropped calls, it is recommended that you include this field.

```
adap.mac,host.devType
00:12:C2:6C:56:74,IP Phone
00:12:C2:D9:46:B0,IP Phone
```

User import

The `user.uid` field is required for this import.

```
user.uid,user.fn,user.ln
Hebert2010, Frank, Hebert
Miller2009, Tammy, Miller
```

Mixed record types import

When combining different record types into a single import file, all of the fields for each record type must exist in the header row. For fields that do not apply to a particular record type, you must still include commas. Required fields for each type must be included.

```
adap.mac,siblings,host.owner,host.devType,user.uid,user.fn,user.ln
,,,Hebert2010,Frank,Hebert
00:12:C2:6C:56:74,,,IP Phone,,,
00:13:CE:6C:56:75,00:13:CE:6C:56:75,Smith2010,Windows,,,
```

Import from a .csv file

To import from a .csv file created in V4.1.1 or higher, see [Import from a previous version on page 109](#) for file format information.

1. Click **Users & Hosts > Hosts**.
2. Click **Import**.
3. Browse to the .csv file containing the items to be imported.
4. Select the file and click **Open**.
5. Click **OK** on the Import window.
6. FortiNAC processes the import file and displays a list of records in the Import Results window. Verify that the data is displaying in the correct columns.
7. Click **OK** to continue the import.

If the required columns are missing or data is not in the correct format, an error message is displayed and the import will not proceed.

If there are no issues with the data, a message is displayed indicating that the import is complete.

Import from a previous version

If you have a .csv file created for or exported from version 4.1.1 or higher, you can import that data into the current version of FortiNAC. You must modify the .csv file so that it conforms to the new import format.

The first row in the .csv file must be a header row and must contain a comma separated list of the database field names that are included in the import file. The order of the fields does not matter, but the order in the header row must match the order of the data contained in the file.

For the names and definitions of the fields that should be used in the header row see [Fields on page 103](#).

Once your .csv file is formatted correctly, see [Import from a .csv file on page 109](#) for import instructions.

Import an administrator

Administrators can be imported into the database from a .csv (comma separated value) file through the administrators view.

Create an import file

To import administrators, create a comma separated value (.csv) file using any text editor or spreadsheet tool. If you are using a text editor to create the file, use commas to separate the fields when you enter the data. Use carriage returns to separate records.

The first row in the file is a header row and must contain a comma separated list of the database field names that are included in the import file. The order of the fields does not matter. For example, to import administrators the header row could have the following fields: `profileName,uid,authType,fn,ln`

Unless otherwise specified, data type is a string with no size limitations. Fields are case sensitive. For example, if you have user IDs SMITH123 and Smith123, the database treats these as two separate user records. If you import something that already exists in the database, the existing record is updated with the new data from the import.



If you import an existing administrator, all fields will be replaced by those in the import file.



When you select the **Make Importable** check box while exporting users, any user with an authentication type of "LDAP" is imported as a local user.

Imported data is displayed on both the administrator user view and the user view. The table below lists all of the possible import data fields by the name that should be used in the header row, indicates which fields are required and provides a definition for each field.

Fields

Field	Required	Definition
profileName	Yes	Admin Profile: Administrators must have an associated admin profile that provides them with permissions for features in FortiNAC. Enter the name of the admin profile that matches an existing profile in the database.
uid	Yes	User ID: Unique alpha numeric user ID. If a directory is used for authentically the FortiNAC database is synchronized with the directory, data for users with matching IDs is overwritten with data from the directory. For example, if you import a user with ID AB118 named Ann Brown and the directory contains a record of AB118 as Andrew Bowman, then your database shows AB118 Andrew Bowman.
authType		Authentication method used for this administrator. Types include: CM: Validates the user to a database on the local FortiNAC appliance.

Field	Required	Definition
		• LDAP: Validates the user to a directory database. FortiNAC uses the LDAP protocol to communicate to an organization's directory. • RADIUS: Validates the user to a RADIUS server.
fn		User's first name.
ln		User's last name.
email		User's e-mail address. For multiple e-mail addresses, enter addresses separated by commas or semi-colons. Messages are sent to all e-mail addresses provided.
addr		User's mailing address.
city		User's city.
st		User's state.
zip		User's postal code.
ph		User's telephone number.
title		User's title.
notes		Notes about this user.
expireDate		Expiration Date: Date that the user is aged out of the database. Date format is MM/dd/yy HH:mm AM/PM Timezone or 04/07/10 08:11 AM EST.
createDate		Creation Date: Date that the user record was created. Date format is MM/dd/yy HH:mm AM/PM Timezone or 04/07/10 08:11 AM EST.
smsNum		Mobile Number: User's mobile phone number. This can be used to send SMS Messages based on events and alarms.
smsPro		Mobile Provider: The carrier or provider for the user's mobile phone. This must match the name of one of the providers in the Mobile Providers list in the database. See Mobile providers on page 1 .

Sample import file

Below is a sample .csv file for importing administrators. The `profileName` and `uid` fields are required.

profileName,uid,authType,fn,ln

Administrator,ajones111,LDAP,,Jones

Administrator,admin111,CM,Admin,User111

Conference Accounts,dpcuser,CM,Elaine,White

Conference Accounts, ajames, CM, james, james

Import IP ranges

Some views in FortiNAC require lists of IP address ranges. An import mechanism is provided to speed up the process of entering this data.

1. Click **System > Settings**.
2. Navigate to the view where you would like to import IP address ranges.
3. Click **Import** at the bottom of the screen.
4. In the **Import** window type the first and last IP address of each range separated by a comma. Press Enter to start a new line. You should not have overlapping ranges or ranges that cross subnets such as 192.168.5.100-192.168.6.150.
5. Click **OK** to import the IP address range.
6. Click **Save Settings** to save your changes.

CLI import tool

If you need to add a set of devices to your FortiNAC database, those devices can be imported from a .csv file using a CLI device import tool. When importing a device, the import tool first checks the database to see if a device with the same IP already exists. If the device exists, then it is removed from the database before the new device is created.

For an SNMP device, the device discovery process determines the device class based on the SNMP MIBs supported by the device. For other device types, the class is based on the import type entered on the CLI command line. You must create a separate .csv file for each device type. For example, if you are importing printers and hubs, the list of printers must be contained within one .csv file and the list of hubs must be contained within another .csv file.

The latest device import tool is located in the `/bsc/campusMgr/bin` directory on the FortiNAC Server.

Device types that can be imported include:

- SNMP
- hub
- WAP
- printer
- server
- pingable
- healthcare
- IPS
- DialUpServer
- StealthWatch
- gaming
- camera
- UPS
- cardReader

- cashRegister
- hvac
- vending
- PBX
- generic
- security
- VPN
- IP phone
- mobile
- network
- toplayer
- Linux
- Unix
- Windows
- macOS

iOS and Android devices cannot be imported with this tool. Use the import options on the Host View instead. See [Import hosts, users or devices on page 102](#).

Create .csv files for device import

Create the CSV file with a text editor, or by exporting the device information from an application that can generate the CSV file format. The file should be formatted as follows for SNMP and non-SNMP devices.



Each device type must be contained within its own .csv file. For example, if you are importing printers and hubs, you must have a .csv file for printers and a separate file for hubs.

SNMP devices

For SNMP devices, format each line in the CSV file as follows:

CONTAINER, IP, USER, TELNET, ENABLE, RWCOMM, ROCOMM, ROLE



There must be a carriage return at the end of the each line in the file. The final line in the CSV file must also end in a carriage return or the last line will not be imported. Also, if a field is null, you must still include the field delimiter (comma).



If multiple SNMP devices with the same name are imported, the first device has the correct name. All subsequent devices are named with a combination of the name and IP address, such as Camera[192.168.5.86].

Settings

Field	Definition
CONTAINER	Folder model in the Inventory. Containers are used to group devices (required). If the Container field is blank, the IP address is used as the Container name and a localhost IP is entered (127.0.0.1).
IP	IP address of the new device (required). If the IP address field is blank, a localhost IP is entered (127.0.0.1).
USER	User name used to telnet into the device.
TELNET	Password used to telnet into the device.
ENABLE	Enable password.
RWCOMM	Read/Write Community Name. This must come first, before the Read Only community name.
ROCOMM	Read Only Community Name.
ROLE	Role for the device.

Example:

```
test,192.168.5.32,admin,net123,,private,public,NAC_Default,
test,192.168.5.35,admin,net456,bscen1,private,public,NAC_Default
```

Non-SNMP devices

For non-SNMP devices, format each line in the CSV file as follows:

```
CONTAINER,IP,NAME,MAC,na,na,na,Role
```



There must be a carriage return at the end of the each line in the file. The final line in the CSV file must also end in a carriage return or the last line will not be imported. Also, if a field is null, you must still include the field delimiter (comma).

Settings

Field	Definition
CONTAINER	Folder model in the Inventory. Containers are used to group devices (required). If the Container field is blank, the IP address is used as the Container name and a localhost IP is entered (127.0.0.1).
IP	IP address of the new device (required). If the IP address field is blank, a localhost IP is entered (127.0.0.1).
NAME	Name of the device.

Field	Definition
	 If multiple non-SNMP devices with the same name are in the import file, the first device has the correct name. All subsequent devices are not imported.
MAC	MAC address of the device (optional).
NA	blank
NA	blank
NA	blank
ROLE	Role for the device.

Import devices with the CLI tool

If you are importing different types of devices, each type must be contained within its own CSV file. For example, to import five printers and two vending machines, you must have a CSV file for the printers and a separate CSV file for the vending machines.

1. Use a secure copy tool to copy the CSV file from your local PC to a TFTP or FTP server.
2. Back up the current FortiNAC database before proceeding.
3. Login to the FortiNAC appliance CLI as admin.
4. Download the CSV file to the FortiNAC's /home/admin directory. Follow the instructions using the applicable KB article:

FTP: See KB article 322956

TFTP: See KB article 281081

5. Run the DeviceImport tool as follows:

```
execute enter-shell
```

```
DeviceImport <absolutePathToImportFile> -type <t>
```

Where:

<absolutePathToImportFile> = The absolute path to the CSV file.

<t> = snmp |hub |wap |printer |server |PINGABLE |healthCare |IPS |Nessus
 |DialUpServer |StealthWatch |gaming |camera |UPS |cardReader |cashRegister
 |hvac |vending |pbx |generic |security |vpn |ipPhone |mobile |network
 |toplayer |linux |unix |windows |macosx

Examples:

```
execute enter-shell
```

```
DeviceImport server.csv -type server
```

```
DeviceImport switches.csv -type snmp
```

6. Log into the FortiNAC.
7. Go to **Network > Inventory** and verify that the devices have been imported. If necessary, modify the device properties.

Import port descriptions

From within the Inventory, you can import port descriptions into the FortiNAC Server and FortiNAC Control Server appliances from a .csv text file containing the comma separated values.

Use only letters, numbers and hyphens (-) when creating port descriptions. Other characters, such as #, may prevent FortiNAC from communicating properly with the device.

1. Create the .csv file with any text editor or spreadsheet tool.

Use commas to separate the data fields if you are using a text editor to create the file. The data you enter into the record for each port must contain all the fields.

Example:

```
"IPAddress","InterfaceID","Floor","Room","Jack"
```

Settings

Field	Description
IPAddress	IP address of the switch.
InterfaceID	ID of the interface. This ID is displayed in Port Properties for the selected port.
Floor	Optional field. If not used, type open and closed quotation marks: "".
Room	Optional field. If not used, type open and closed quotation marks: "".
Jack	Optional field. If not used, type open and closed quotation marks: "".

2. Save the file with the .csv extension in the filename.
3. Click **Network > Inventory**.
4. Right-click the **Customer Container** and select **Import Port Desc.**
5. Navigate to the directory where the .csv file containing the port descriptions is located. Click to select the file, then click **Open**.

The port description data is imported into FortiNAC.

Export data



Export Data functionality may not be available in some views.

Export data to a CSV file, an Excel spreadsheet, or an RTF document. Select from a list of possible fields and control the order of the data in the export. If you plan to re-import the same file after editing it, you must use a CSV file. See [Import hosts, users or devices on page 102](#) for a list of fields that can be exported or imported and their definitions.

1. Navigate to a View with export options, such as the Host View.
2. Use the Search or Filters to display a list of records.
3. Use Ctrl-click or Shift-click to select the records you wish to export. If you do not select specific records, all displayed records are exported. When the Export dialog is displayed, check the Selected Rows check box to export only selected records.
4. At the bottom of the window, click the icon for the type of export file needed, such as PDF.
5. In the File Name field, enter a name for the export file. Do not add an extension. It is added when you click OK based on the file type you selected in the previous step.
6. The fields contained in the Export Dialog vary based on the View from which you are exporting.
7. Select the field(s) you want to export and click the right-arrow to move the field to the Show As Columns list. Ctrl-click to select more than one field at a time.
8. Click the double-arrows to move all of the fields from one column to the other.
9. To remove fields from the export, select them in the Show As Columns list and click the left-arrow.
10. To reorder the fields in the **Show As Columns** list, click the field and then click the Up or Down arrows. The order displayed from top to bottom corresponds to the columns in the export from left to right. For example, if the first field at the top of the list is Last Name, that is the left most column in the export.
11. To sort fields alphabetically, click **Sort** labeled AZ.
12. Check the **Selected Rows** check box to export only the records selected in the View. If you leave this box unchecked, all the records in the View are exported.
13. A Header line consisting of the field names is inserted in the .csv file if you check either or both of the **Make Importable** check boxes. In addition, the fields required for import are automatically added to your export.



When you select the **Make Importable** check box while exporting users, any user with an authentication type of "LDAP" is imported as a local user.



Only the Export Dialog accessed from Users, Hosts or Adapters views includes two Make Importable check boxes because of the relationship between Users and their corresponding Hosts. The Export Dialog accessed from other views may have one Make Importable check box, such as administrators, or no Make Importable check boxes, such as Connections.

-
14. Click **OK**.
 15. Depending on your browser, the file is either generated and saved to a downloads location or you may need to navigate to the **location** where the file is to be placed.

Users & Hosts

The **Users & Hosts** menu contains the views and controls for accounts and devices.

Administrators	119
Administrator profiles	125
Guests & Contractors	151
Account requests	191
Registration requests	192

Administrators

FortiNAC's administrator system allows you to organize admins to better delegate work and also to limit which admins have what kind of access. On this page, you can add admins, edit them, and apply an Admin Profile. (See: [Administrator profiles](#)). An Admin Profile is a highly useful profile that you can create to determine what kind of privileges you, as the supervising System Administrator, want to give them.

Simply go to the Profiles tab under **Users & Hosts > Administrators**.

Some examples include Help Desk, Operator, Security Analyst, etc. This differentiation of admin types allows your team to work together while maintaining segmentation of data access. The process can be automated, too. You can well imagine how it might be helpful to automatically apply profiles for a very large number of temporary administrators for a conference, whose privileges should expire after a certain time period that you determine.

The profiles are ranked, so that you won't run into the problem of one user having two profiles. The user will automatically be assigned the top profile.

Here's some things you should know:

- When adding Administrator accounts to the FortiNAC Manager, be sure these accounts also exist on the managed FortiNAC Servers so the Administrator users can have access to the data. **Important:** Account must use the same password on both Manager and FortiNAC Server.
- If you're the System Administrator, you cannot delete your account, as you control everything.
- The underlying administrators can't select their own profile. The profile is forced upon them.
- If you want to use a different profile, then you have to use a different account.
- If there are more than 1000 administrators in the database, the users are not automatically displayed. Large numbers of records may load slowly if not filtered.
- Admin user accounts for appliance CLI access are independent of the Administrator users for UI access. CLI users are not listed in the UI.
- To modify passwords for UI and appliance CLI accounts, see [Passwords](#).
- For details on FortiNAC-OS CLI admin users, see "Admin user" section in the [CLI Reference manual](#).
- FortiNAC supports up to 50 simultaneous administrators logins.

Note: Administrators are also network users, therefore, FortiNAC also displays them in the Users View.

Settings

Fields used in filters are also defined in this table.

Field	Definition
Add Filter	Allows you to select a field from the current view to filter information. Select the field from the drop-down list, and then enter the information you wish to filter. See Filters on page 34 .
Update	Displays the filtered data in the table.
Administrators	
User ID	Unique alphanumeric ID for this user. Required.

Field	Definition
First Name	User's first name.
Last Name	User's last name. Required.
Admin Profile	Administrators must have an associated administrator profile that provides them with permissions for features in FortiNAC. Click the link in the administrators table for the selected user to go to the profile displayed. See Administrator profile on page 174 .
Auth Type	Authentication method used for this administrator. Types include: • Local: Validates the user to a database on the local FortiNAC appliance. • LDAP: Validates the user to a directory database. FortiNAC uses the LDAP protocol to communicate to an organization's directory. • RADIUS: Validates the user to a RADIUS server.
E-mail	E-mail address used to send system notifications associated with features such as alarms or profiled devices.
Phone	Optional demographic information.
Address	
City	
State	
Postal Code	
Title	
Mobile Number	Mobile Phone number used for sending SMS messages to administrators.
Mobile Provider	Mobile provider for the mobile phone number entered in the previous field. Used to send SMS messages to administrators. This field also displays the format of the SMS address that will be used to send the message. For example, if the provider is US Cellular, the format is xxxxxxxxx@emai.uscc.net, where the x's represent the user's mobile phone number. The number is followed by the email domain of the provider's message server.
User Expires	The user is deleted from the database when the date specified here has passed. The date is automatically calculated based on the information entered when Aging is configured. The default setting for administrators is blank or Never Expire. Administrators may or may not have an expiration date depending on how the account was created. See Aging out host or user records on page 241 and Set user expiration date on page 208 . Administrators assigned the System Administrator profile cannot be aged out.
User Inactivity Date	Controls the number of days a User is authorized on the network. User is deleted from the database when the date specified here has passed. The date is continuously recalculated based on the information entered in the Days Inactive field. See Aging out host or user records on page 241 .
User Inactivity Limit	Number of days the user must remain continuously inactive on the network to be removed from the database. See Aging out host or user records on page 241 .
Last Login/Logout	Date of the last time the user logged into or out of the network or the FortiNAC admin UI. This date is used to count the number of days of inactivity.

Field	Definition
Last Modified By	User name of the last user to modify the administrator.
Last Modified Date	Date and time of the last modification to this administrator.
Right click menu options	
Copy	Copy the selected User to create a new record.
Delete	Deletes the selected User.
Group Membership	Displays groups in which the selected user is a member. Administrators are also regular users, therefore, separate options are displayed for administrator groups and user groups. Options are Group Membership (User) and Group Membership (Administrator) .
Groups	Displays groups in which the selected user is a member. See Group membership on page 151 .
Modify	Opens the Modify User window for the selected profile.
Set Admin Profile	Allows you to modify the administrator profile for one or more users. This also allows you to remove the "Administrator" Profile for a user without the need to first delete and then recreate the user. See Modify an administrator profile on page 124
Set Expiration	Launches a tool to set the date and time for the user to age out of the database. See Set user expiration date on page 208 .
Edit Theme	Opens the User Theme dialog and allows you to modify the look and feel of the user interface for each administrator.
Import/Export	Import and Export options allow you to import users into the database from a CSV file or export a list of selected hosts to CSV, Excel, PDF, or RTF formats. See Import an administrator on page 109 and Export data on page 116 .

Add an administrator

If you are creating administrators to manage guests or devices, you must create an administrator who has the appropriate administrator profile associated. See [Administrator profiles on page 125](#).

1. Select **Users & Hosts > Administrators**.
2. Click **Add**.
3. Enter a **User ID** for the new administrator and click **OK**.

As you enter the user ID, the network user database is checked to see if there is a current user with the same ID and a drop-down list of matching users is displayed. If you enter an ID that already exists as a regular network user, the network user and the administrator become the same person with a single account.

This allows you to give a network user administrator privileges to help with some administrative tasks.

4. Use the table of below to complete the information in the **Add User** dialog:

Field	Definition
Authentication Type	Authentication method used for this administrator. Types include: • Local: Validates the user to a database on the local FortiNAC appliance.

Field	Definition
	• LDAP: Validates the user to a directory database. FortiNAC uses the LDAP protocol to communicate to an organization's directory. • RADIUS: Validates the user to a RADIUS server.
Admin Profile	Profiles control permissions for administrators. See Administrator profiles on page 125. Add: Opens the administrator profiles window allowing you to create a new profile without exiting the Add User window. Modify: Allows you to modify the selected administrator profile. Note that modifications to the profile affect all administrators that have been assigned that profile.
User ID	Unique alphanumeric ID for this user.
Password	Password used for local authentication. Note: You cannot view the password of the administrator you have created.  If you authenticate users through LDAP or RADIUS, the password field is disabled and the user must log in with his LDAP or RADIUS password.
First Name	User's first name.
Last Name	User's last name.
Address	Optional demographic information.
City	
State	
Zip/Postal Code	
Phone	
E-mail	E-mail address used to send system notifications associated with features such as alarms or profiled devices. Also used to send Guest self registration requests from guests requesting an account. For multiple e-mail addresses, enter addresses separated by commas or semi-colons. Messages are sent to all e-mail addresses provided.
Title	User's title, such as Mr. or Ms.
Mobile Number	Mobile Phone number used for sending SMS messages to administrators.
Country Code	The country code of the mobile phone number.

Field	Definition
Mobile Provider	Mobile provider for the mobile phone number entered in the previous field. Used to send SMS messages to administrators. This field also displays the format of the SMS address that will be used to send the message. For example, if the provider is US Cellular, the format is xxxxxxxxx@email.uscc.net, where the x's represent the user's mobile phone number. The number is followed by the email domain of the provider's message server.
Notes	Free form notes field for additional information.
Multi-Factor Authentication	Select None to disable Multi-Factor Authentication. Select SMS to activate sending a one-time token code through SMS to the mobile number with a mobile provider selected. Select Email to activate sending a one-time token code to the e-mail address provided. For more details on Multi-Factor Authentication, please see Multi-factor Authentication on page 903.
User Never Expires	If enabled, administrators are never aged out of the database. The default is enabled.  Administrators assigned the System Administrator profile cannot be aged out.
Propagate Hosts	The Propagate Hosts setting controls whether or not the record for the host owned by the user is copied to all managed FortiNAC appliances. This field is only displayed if the FortiNAC server is managed by a FortiNAC Control Manager.

- Click **OK** to save the new user.

Modify an administrator

Administrators cannot select a different administrator profile for their own account. Use a second administrator account to select a different profile.

- Select **Users & Hosts > Administrators**.
- Select a user from the list.
- Click **Modify**.
- On the **Modify User** window, edit your data as needed.
- Click **Change Password** to modify this user's password. This option is only available if the user is set for Local authentication. Users who authenticate through the directory or a RADIUS server must change their passwords in the directory or RADIUS server directly.
- Click **OK** to save your changes.

For information on individual fields, see [Add an administrator on page 121](#).

Delete an administrator

1. Select **Users & Hosts > Administrators**.
2. Select a user from the list.
3. Click **Delete**.
4. A message is displayed asking if you are sure. Click **OK** to continue.

You are asked if you would like to delete registered hosts. If the administrator is also the owner of any registered hosts, it is recommended that you delete the registered hosts. If they are not deleted, registered hosts associated with a deleted user become registered devices. If a user connects to the network with one of these devices, there is nothing to prevent network access because the device is known in the database.

Copy an administrator

You may copy a user, save it under another name, and use it as the basis for a new user.

1. Click **Users & Hosts > Administrators**.
2. The **Admin Users** window opens with a list of current users.
3. Select the user and click, **Copy**.
4. In the **User ID** window displayed, enter an alphanumeric ID for the new administrator and click **OK**. As you enter the user ID, the network user database is checked to see if there is a current user with the same ID and a drop-down list of matching users is displayed. If you enter an ID that already exists as a regular network user, the network user and the administrator become the same person with a single account.
This allows you to give administrator privileges to a network user to help with some administrative tasks.
5. Change the name of the user, or other information and parameters.
6. Click **OK**.

Modify an administrator profile

You can modify the administrator profile for one or multiple users at a time. This also allows you to remove the "Administrator" Profile for a user without the need to first delete and then recreate the user.

1. Select **Users & Hosts > Administrators**.
2. Select one or more users from the list.
3. Right-click and select **Set Admin Profile**.
4. Select the **Admin Profile** from the drop-down list.
5. Click **Add** to add a new profile or **Edit** to modify the selected profile.
6. Click **OK**.

Administrator profiles

Administrator profiles are templates assigned to administrators to define what a user can do in FortiNAC. Every administrator is required to have an administrator profile. An administrator profile can be assigned to more than one administrator.

Each administrator profile contains a list of permissions that are inherited by the associated administrators. Permissions configured in administrator profiles control the views in FortiNAC that can be accessed. If permission for access is given, in most cases, the administrator can Add/Modify and Delete data.



If an administrator profile in use is changed, the changes do not take effect until the associated administrators log out of FortiNAC and log in again.

Custom setting

For guest manager or device profiler, advanced permissions control items such as the guest account templates that can be used by someone with permission for guest/contractor accounts.

Landing page

Administrator profiles also designate the first screen or landing page displayed when the administrator logs into FortiNAC, days and times that users can log in and the number of minutes of inactivity that trigger an automatic logout. Due to the complexity of the permissions structure, it is recommended that you define the job functions of your administrators to ensure that you have considered the permissions required for each administrator profile.

Profile mapping

You can create profiles for groups of administrators so that new administrators are automatically added with your specified configurations. If administrator profile mapping is configured, moving an administrator to a group which is mapped changes the administrator to fit the group's profile. See [Mappings process on page 145](#) for additional information.

System Administrator

The **System Administrator** profile is a default system profile. See [Default administrator profiles on page 126](#).

Settings

Field	Definition
Name	User specified name for the profile. This name is displayed in the administrator window when you are attaching the profile to an administrator.
Inactivity Time	User is logged out after this amount of time has elapsed without any activity.

Field	Definition
Login Availability	Indicates when users with this profile can log in to FortiNAC. Options include: Always or Specify Time. If you choose Specify Time, the user is limited to certain times of day and days of the week.
Landing Page	Indicates the first view displayed when an administrator with this profile logs into FortiNAC.
Note	User specified note field. This field may contain notes regarding the data conversion from a previous version of FortiNAC
Lock Out After Attempts	Indicates the number of allowed login attempts before the user is locked out.
Lock Out Duration	Indicates the amount of time a user is locked out before another login attempt is allowed.
Last Modified By	User name of the last user to modify the profile.
Last Modified Date	Date and time of the last modification to this profile.
Right click options	
Copy	Copy the selected Profile to create a new record. The Administrator Profile cannot be copied.
Delete	Deletes the selected Profile. Profiles cannot be deleted if they are in use. The Administrator Profile can never be deleted.
Modify	Opens the Modify Admin Profile window for the selected profile. On the administrator profile, only the Inactivity Time can be modified.
In Use	Opens a list of administrators that have the selected profile attached.
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746 .
 You must have permission to view the admin auditing log. See Add an administrator profile on page 139.	

Default administrator profiles

FortiNAC has some default profiles that can be used to control system access. These profiles are always included in the database. They can be modified, deleted or copied.

Default profiles - new database

The table below describes the profiles that are in any new FortiNAC database and the default settings for each profile.

View	Access	Permissions enabled
System Administrator		

View	Access	Permissions enabled
All	This profile cannot be deleted or copied. The only attribute of this profile that can be modified is the Inactivity Time. The System Administrator profile has access to every part of FortiNAC.	All
Help desk		
Group Membership	User can access the group membership for Hosts and add or modify the selected host's membership in groups.	Access
Guest/Contractor Accounts	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete
Locate Hosts & Users	User can search for Hosts and Users but cannot modify data. This is the default landing page when a user with this profile logs into FortiNAC.	Access
Self Registration Requests	User can view self registration requests and allow or deny those requests.	Access Add/Modify
Operator		
Group Membership	User can access the group membership for Hosts and add or modify the selected host's membership in groups. Operators are restricted to the host and user groups they are configured to manage. They do not have access to all hosts and users	Access Add/Modify
Locate Hosts & Users	User can view adapter, host, user, and device identity. User can modify Host information but cannot delete any records.	Access
Manage Hosts & Ports	• Adapter List: Disable adapters. • Adapter Properties: View only. • Host Properties: View and modify access, but cannot send a message. • User Properties - View Only. • Device Identity - View and export data. This is the default landing page when a user with this profile logs into FortiNAC.	Access
Guest/Contractor Accounts	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete
Self Registration Requests	User can view self registration requests and allow or deny those requests.	Access Add/Modify
Profile_Sample		
Group Membership	User can access the group membership for Hosts and add or modify the selected host's membership in groups.	Access Add/Modify
Guest/Contractor Accounts	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Custom Settings

View	Access	Permissions enabled
	User is limited to the GuestAccess_Sample template, can create accounts 45 days in advance and can create accounts with a maximum duration of 15 days.	
Self Registration Requests	User can view self registration requests and allow or deny those requests.	Access Add/Modify
Security analyst		
Dashboard	User can access and view the dashboard.	Access
Network Devices	User can view, add, modify, or delete network devices in the following views: • CLI configuration • Device profiling rules • L2 polling • L3 polling • Locate • Port changes • Topology	Access Add/Modify Delete
Users/Hosts/ Adapters	User can access, add, modify, or delete users, hosts, and adapters in the following views: • Adapters View • Connections • Device Identity • Hosts View • Scan Results • Users View	Access Add/Modify Delete

Possible profiles - upgraded database

Prior versions of FortiNAC contained several user types with varying permissions. From Version 7.0 forward there is only one type of administrator and access is controlled based on the settings of the administrator profile associated with each user. During the upgrade process any existing administrator types and their corresponding permissions are converted to administrator profiles and assigned to administrators. There may be many as two Help Desk profiles and eight Operator profiles created during the upgrade. The table below contains the full list of administrator profiles that could be created.

View	Access	Permissions enabled
Administrator		
All	This profile cannot be deleted or copied. The only attribute of this profile that can be modified is the Inactivity Time. The System Administrator profile has access to every part of FortiNAC.	All
Help desk		
Group Membership	User can access the group membership for Hosts and add or modify the selected host's membership in groups.	Access
Guest/Contractor Accounts	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete

View	Access	Permissions enabled
Locate Hosts & Users	User can search for Hosts and Users but cannot modify data. This is the default landing page when a user with this profile logs into FortiNAC.	Access
Self Registration Requests	User can view self registration requests and allow or deny those requests.	Access Add/Modify
Help desk with messaging		
Group Membership	User can access the group membership for Hosts and add or modify the selected host's membership in groups.	Access
Guest/Contractor Accounts	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete
Locate Hosts & Users	User can search for Hosts and Users but cannot modify data. This is the default landing page when a user with this profile logs into FortiNAC.	Access
Send Message	User can send messages to hosts with the Persistent Agent or Mobile Agent installed.	Access
Self Registration Requests	User can view self registration requests and allow or deny those requests.	Access Add/Modify
Operator		
Group Membership	User can access the group membership for Hosts and add or modify the selected host's membership in groups. Operators are restricted to the host and user groups they are configured to manage. They do not have access to all hosts and users	Access Add/Modify
Locate Hosts & Users	User can view adapter, host, user, and device identity. User can modify Host information but cannot delete any records.	Access
Manage Hosts & Ports	Adapter List - Disable adapters. Adapter Properties- View only. Host Properties-View and modify access, but cannot send a message. User Properties - View Only. Device Identity - View and export data. This is the default landing page when a user with this profile logs into FortiNAC.	Access
Guest/Contractor Accounts	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete
Self Registration Requests	User can view self registration requests and allow or deny those requests.	Access Add/Modify
Operator with messaging		
Group Membership	User can access the group membership for Hosts and add or modify the selected host's membership in groups.	Access Add/Modify

View	Access	Permissions enabled
Locate Hosts & Users	User can view adapter, host, user, and device identity. User can modify Host information but cannot delete any records.	Access
Manage Hosts & Ports	• Adapter List - Disable adapters. • Adapter Properties- View only. • Host Properties-View and modify access, and can send a message. • User Properties-View Only. • Device Identity - View and export data. This is the default landing page when a user with this profile logs into FortiNAC.	Access
Guest/Contractor Accounts	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete
Self Registration Requests	User can view self registration requests and allow or deny those requests.	Access Add/Modify
Send Message	User can send messages to hosts with the Persistent Agent installed.	Access
Operator with add hosts		
Group Membership	User can access the group membership for Hosts and add or modify the selected host's membership in groups.	Access Add/Modify
Locate Hosts & Users	User can view adapter, host, user, and device identity. User can modify Host information but cannot delete any records.	Access
Manage Hosts & Ports	• Adapter List - Disable adapters. • Adapter Properties- View only. • Host Properties-View and modify access, but cannot send a message. • User Properties-View only. • Device Identity - View and export data. • User can add hosts. This is the default landing page when a user with this profile logs into FortiNAC.	Access Add/Modify
Guest/Contractor Accounts	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete
Self Registration Requests	User can view self registration requests and allow or deny those requests.	Access Add/Modify
Operator with delete hosts		
Group Membership	User can access the group membership for Hosts and add or modify the selected host's membership in groups.	Access Add/Modify
Locate Hosts & Users	User can view adapter, host, user, and device identity. User can modify Host information and delete host and adapter records.	Access
Manage Hosts & Ports	• Adapter List - Disable adapters. • Adapter Properties- View only.	Access

View	Access	Permissions enabled
	- Host Properties-View and modify access, but cannot send a message. - User Properties-View only. - Device Identity - View and export data. This is the default landing page when a user with this profile logs into FortiNAC.	Delete
Guest/Contractor Accounts	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete
Self Registration Requests	User can view self registration requests and allow or deny those requests.	Access Add/Modify
Operator with add hosts and messaging		
Group Membership	User can access the group membership for Hosts and add or modify the selected host's membership in groups.	Access Add/Modify
Locate Hosts & Users	User can view adapter, host, user, and device identity. User can modify Host information but cannot delete any records.	Access
Manage Hosts & Ports	- Adapter List - Disable adapters. - Adapter Properties- View only. - Host Properties-View and modify access, and can send a message. - User Properties-View only. - Device Identity - View and export data. - User can add hosts. This is the default landing page when a user with this profile logs into FortiNAC.	Access Add/Modify
Guest/Contractor Accounts	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete
Self Registration Requests	User can view self registration requests and allow or deny those requests.	Access Add/Modify
Send Message	User can send messages to hosts with the Persistent Agent installed.	Access
Operator with delete hosts and messaging		
Group Membership	User can access the group membership for Hosts and add or modify the selected host's membership in groups.	Access Add/Modify
Locate Hosts & Users	User can view adapter, host, user, and device identity. User can modify Host information and delete host and adapter records.	Access
Manage Hosts & Ports	- Adapter List - Disable adapters. - Adapter Properties- View only. - Host Properties-View and modify access, and can send a message. - User Properties-View only. - Device Identity - View and export data.	Access Delete

View	Access	Permissions enabled
	This is the default landing page when a user with this profile logs into FortiNAC.	
Guest/Contractor Accounts	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete
Self Registration Requests	User can view self registration requests and allow or deny those requests.	Access Add/Modify
Send Message	User can send messages to hosts with the Persistent Agent installed.	Access
Operator with delete hosts, add hosts, and messaging		
Group Membership	User can access the group membership for Hosts and add or modify the selected host's membership in groups.	Access Add/Modify
Locate Hosts & Users	User can view adapter, host, user, and device identity. User can modify Host information and delete host and adapter records.	Access
Manage Hosts & Ports	• Adapter List - Disable adapters. • Adapter Properties- View only. • Host Properties-View and modify access, and can send a message. • User Properties-View only. • Device Identity - View and export data. • User can add hosts. This is the default landing page when a user with this profile logs into FortiNAC.	Access Add/Modify Delete
Guest/Contractor Accounts	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials.	Access, Add/Modify Delete
Self Registration Requests	User can view self registration requests and allow or deny those requests.	Access Add/Modify
Send Message	User can send messages to hosts with the Persistent Agent installed.	Access
Profile_Sample		
Group Membership	User can access the group membership for Hosts and add or modify the selected host's membership in groups.	Access Add/Modify
Guest/Contractor Accounts	User can add, modify or delete guest accounts, send email and SMS messages to guests with their credentials. User is limited to the GuestAccess_Sample template, can create accounts 45 days in advance and can create accounts with a maximum duration of 15 days.	Access, Add/Modify Custom Settings
Self Registration Requests	User can view self registration requests and allow or deny those requests.	Access Add/Modify
Security analyst		
Dashboard	User can access and view the dashboard	Access

View	Access	Permissions enabled
Network Devices	User can view, add, modify, or delete network devices in the following views: • CLI configuration • Device profiling rules • L2 polling • L3 polling • Locate • Port changes • Topology	Access Add/Modify Delete

Permissions list

Administrator profiles contain permissions settings. An administrator inherits permissions from the administrator profile applied to his user account. The table below contains a list of the permissions that can be set in an administrator profile and any special information about each setting.

Access levels

Level	Definition
Access	If enabled, the user will be able to see data in the views shown in the Permission Set, but not add, modify or delete. There are some exceptions to this that are noted in the table of permissions. In some cases, by enabling Access, other permissions are automatically enabled. For example, if you enable Access for guest/contractor accounts, Add/Modify and Delete are automatically enabled and cannot be disabled.
Add/Modify	If enabled, the user can add or modify data in the views shown in the Permission Set.
Delete	If enabled, the user can delete data in the views shown in the Permission Set.
Custom	If enabled, an additional tab is shown that contains advanced settings for the Permission Set. For example, if Access to guest/contractor accounts is enabled and Custom is enabled, advanced options can be set on the Manage Guests tab.

Permissions list

Where applicable, this table assumes that Access, Add/Modify, Delete and Custom options are enabled.

Views	Permissions	Notes
Admin auditing		
Admin Auditing	Provides access to the admin auditing log.	
Admin profiles		
Admin profiles	Provides access to admin profiles.	
Config wizard		

Views	Permissions	Notes
Config wizard	Provides access to config wizard.	
Dashboard		
Dashboard	Provides access to the dashboard tiles. Tiles require additional permissions as follows: • Alarms Panel: Requires access to Event/Alarm, links and buttons are enabled if Add/Modify is enabled. Note: Events/Alarms permissions are located under the Logs permission group. • Summary Panel: Requires access to System Settings. • Network Device Summary Panel: Requires access to Devices, links are enabled if Add/Modify or Delete are enabled for Devices. • Host Summary Panel: Requires access to Users/Hosts/Adapters. • Scans Panel—Requires access to Policy. • User Summary Panel—Requires access to Users/Hosts/Adapters. • License Information Panel—Requires access to System Settings. • Persistent Agent Summary Panel—Requires access to Policy. • Performance Summary Panel—Requires access to Event/Alarm.	Requires that other permissions be selected to display associated tiles.
Event/alarm management		
Event to Alarm Mappings	If enabled, the views shown in the left column can be accessed.	Reports can be accessed but not all options can be used without access to User/Host/Adapter being enabled.
Event Management		
Group membership		
Group Membership	Allows access to Host, User, Device or Port group membership. Requires that one of the following additional permissions be enabled: • Devices • Locate Hosts & Users • Manage Hosts & Ports • Users/Hosts/Adapters	
Groups		
Groups	If enabled, allows access to the Groups View where you can view, add, modify or delete a group.	
Guest/Contractor Accounts		

Views	Permissions	Notes
Guest/Contractor Accounts	If enabled, allows access to the Guest Contractor Accounts View where you can view, add, modify or delete a guest account.	Has a Custom option that enables the Manage Guests Tab.
Custom/Manage Guests	This tab displays when the Custom permission is enabled. Custom Options include: • Guest Account Access: Indicates whether user can access All, Own or No guest accounts after they have been created. • Account Types: Allows user to create Individual, Bulk and or Contractor accounts • Create Accounts Days in Advance (Maximum): Number of days before guest registers that the account can be created. • Create Accounts Active For Days (Maximum): Maximum number of days that accounts created by this user are allowed to be active. • Allowed Templates: Templates that can be used to create guest accounts Refer to Add a guest manager profile for detailed information.	
Hosts		
Adapters view	Provides access to Hosts views.	
Application view		
Endpoint fingerprints		
FortiGate sessions		
Hosts view		
Incoming events parser	Provides access to incoming events parser.	
Locate hosts & users		
Locate Hosts & Users	If enabled, the views shown in the column on the left can be accessed. • User can view adapter, host, user, and device identity. • User can view group membership for Hosts and Users. • User can modify Host information including registering a host. • User can modify User properties for network users and administrators. • User can delete Host and Adapter records.	
Logs		
Alarms	If enabled, the views shown in the column on the left can be accessed.	
Connections		
Events	Users can view information about events within the system and on the network.	
Scan Results		

Views	Permissions	Notes
Manage hosts & ports		
Manage Hosts & Ports	If enabled, the views shown in the column on the left can be accessed. Access is limited to users, hosts and adapters in groups for which user has permission. See Limit user access with groups on page 846. User can view adapter, host, user, and device identity. User can modify Host information including registering a host. User can modify User properties for network user. User can enable or disable an adapter. User can view Port properties for the ports where an adapter is connected.	
Network devices		
Network Device Summary Dashboard Tile CLI Configuration Device Profiling Rules L2 Polling L3 Poling Locate Port Changes Inventory	If enabled, the views shown in the left column can be accessed.	To see Profiled Devices that option must be enabled separately.
Policy		
Authentication Policy Endpoint Compliance Policy Network Access Policy Network Device Roles Persistent Agent Properties Policy Configuration Portal Policy Remediation Configuration Roles Security Actions Supplicant EasyConnect Policy	If enabled, the views shown in the left column can be accessed. Add/Modify & Delete permissions are enabled by default and cannot be modified. The Passive Agent registration view requires access to Groups to add or modify Passive Agent Configurations.	
Portal configuration		
Portal Configuration Portal SSL Request Processing Rules	If enabled, allows the user to view and edit settings for portals. Users with the Policies permission set enabled will also have this permission set enabled. Custom options include:	

Views	Permissions	Notes
	• Access: Allows the user to view the portal settings. • Add/Modify: Allows the user to view the settings, add new portal settings, and delete existing portal configurations. Requires that Access permissions be enabled. Permissions can be further modified to prevent the user from adding new portal configurations or modifying the default portal configuration. • Delete: Allows the user to view portal settings, add new ones, and modify and delete existing portal configurations. Requires that Add/Modify permissions be enabled.	
Profiled devices		
Profiled Devices	If enabled, allows the user to view the list of profiled devices. User can also Export devices, register a device, enable or disable a device, delete the device from the list and view details and notes for a selected device. The Views column on the Profiled Devices View contains icons that provide access to details about the selected device. these icons only display if additional permissions are enabled for the administrator. Possible views include: Adapter Properties, group membership, port properties and Device Properties. Adapter Properties: Requires permission for users, hosts, and adapters. Group Membership: Requires permission for group membership. Port Properties: Requires permission for Devices. Device Properties: Requires permission for users, hosts, and adapters or Devices.	Has a Custom option that enables the Profile Devices Tab.
Custom/Profile Devices	This tab displays when the Custom permission is enabled. Custom Options include: • Register, Delete, and Disable Profiled Devices: If enabled, the user can register, delete and disable devices that have been profiled by device profiler. • Modify Device Rule Confirmation Settings: If enabled, the user can change rule confirmation settings on devices that have been profiled by device profiler. Rule confirmation settings control whether or not device profiler checks a previously profiled device to determine if it still meets the criteria of the rule that	

Views	Permissions	Notes
	categorized the device. • Manage Profiled Devices Using These Rules: • All Rules: includes current rules and any rules created in the future. • Specify Rules: you must choose the rules from the Available Rules field and manually move them to the Specify Rules field. • Available Rules: Shows the existing rules you can select for this profile. Select the rule and click the right arrow to move it to the Selected Rules pane. • Selected Rules: Shows the rules you selected from the Available Rules section. The user can only access the devices associated with the rules in this list. Refer to for detailed information.	
RADIUS		
Local RADIUS Service	Provides access to RADIUS views.	
RADIUS Attribute Groups		
RADIUS Proxy		
Windbind Configuration		
Reporting		
Analytics	If enabled, the views shown in the left column can be accessed.	
Reports		
Security logs		
Security Alarms	If enabled, the views shown in the left column can be accessed.	This permission set is only available when Security Incidents is enabled within your current license package.
Security Events	User has access to view security alarms created when a security rule is matched. Users can take action on a security alarm if it was not done automatically. The user's administrator profile settings determine the actions they are allowed to complete.	Has a Custom option that enables the Security Events tab.
Security rules		
Security Actions	If enabled, the views shown in the left column can be accessed.	This permission set is only available when Security Incidents is enabled within your current license package.
Security Rules	User can create security devices, and security event rules. Users will establish and maintain all rules and the default actions associated with each rule.	
Security Triggers		
Self registration requests		
Self Registration Requests	If enabled, user can manage requests for network access submitted by Guests from the captive portal.	
Host Registration Requests		
Send message		

Views	Permissions	Notes
Send Message	User can send messages to hosts with the Persistent Agent or Mobile Agent installed.	
Service connectors		
Service connectors	Provides access to service connectors.	
Shared host filters		
Shared host filters	Provides access to shared host filters.	
System settings		
Scheduler	If enabled, the views shown in the left column can be accessed.	All settings can be accessed when this permission is enabled. Refer to Settings on page 863 for a complete list.
Settings		
Certificate Management		
Network Settings		
System Settings		
User Settings		
Users/hosts/adapters		
Adapters View	If enabled, the views shown in the left column can be accessed.	
Device Identity		
Hosts View		
Users View		

Add an administrator profile

Administrator profiles control permissions for administrators.

1. Click **Users & Hosts > Administrators > Profiles**.
2. Click **Add**. The **Add Admin Profile** screen appears with the **General** tab highlighted.
3. Enter a name for the profile.
4. Use the table below to configure the new administrator profile.
5. On the **Permissions** tab note that some permissions are dependent on each other. Refer to the [Permissions list on page 133](#) for additional information.
6. Click **OK** to save.

General tab settings

Field	Definition
Name	Enter a name that describes the profile, such as librarian or IT staff.
Login Availability	Indicates when users with this profile can log in to FortiNAC. Options include: Always or Specify Time . If you choose Specify Time , user access to FortiNAC is limited to certain times of day and days of the week.
Logout After ... Minutes of Inactivity	User is logged out after this amount of time has elapsed without any activity in the user interface.

Field	Definition
Lock Out After...failed attempts	User is locked out after this amount of allowed failed attempts.
Lock Out Duration...seconds	User is locked out for this amount of time before another login attempt is allowed.
Manage Hosts And Ports	Restricts an administrator to a specific set of hosts or ports. The set is defined by host and port groups that are assigned to be managed by a specific group of administrators. Any administrator that has a profile with this option enabled can only view and or modify a subset of the data in FortiNAC. Typically, this type of user would only have the Manage Hosts & Ports permission set on the Permissions tab, therefore, this setting is not used frequently. Default = All. • All: All groups containing hosts and ports can be accessed. • Restrict By Groups: Enables the restriction of administrators to specific hosts and ports. For an overview and additional setup information, see Limit access with groups on page 148.
Note	User specified note field. This field may contain notes regarding the data conversion from a previous version of FortiNAC for an existing administrator profile record.
Enable Guest Kiosk	If you enable this mode, the ONLY thing that the administrator can access is the self-service Kiosk. Everything else in FortiNAC is disabled. The administrator can log into FortiNAC to provide visitors self-serve account creation through a kiosk. For added security, use a kiosk browser.
Kiosk Template	Field displays only if Enable Guest Kiosk is selected. Select a kiosk template for this administrator profile. All visitors who use the self-service kiosk when this administrator is logged in are assigned this guest template.
Kiosk Welcome Message	Field displays only if Enable Guest Kiosk is selected. Enter the message that will appear when the kiosk user creates a guest account.

Permissions tab settings

Field	Definition
Landing Page	Indicates the first view displayed when an administrator with this profile logs into FortiNAC. There are no options displayed in this field until permissions are selected.
Permission Set	Click the arrow next to a permission set to see the Views that can be accessed when this permission set is enabled. For example, if Devices is selected, this profile provides access to the following: CLI configuration, device profiling rules, L2 Polling, L3 Polling, Locate, Port Changes, and Topology
Access	Indicates that the user will have view access to the permission set in the left column. Depending on the permission set, enabling Access automatically enables Add/Modify and/or Delete.

Field	Definition
Add/Modify	Indicates that the user will be able to add or modify records in the permission set in the left column.
Delete	Indicates that the user will be able to delete records in the permission set in the left column.
Custom	When Custom is enabled for a permission set an addition tab is displayed. For example, if Custom is enabled for Guest Contractor Accounts , a Manage Guests tab is displayed allowing you to configure additional controls for guest account creation. See Add a guest manager profile on page 175 for information on the Manage Guest tab. See Profiles for device managers on page 256 for information on the Profile Devices tab.
Check All Uncheck All Buttons	Checks or unchecks all permissions.

Specify login availability time

This option allows you to limit access to FortiNAC for an administrator based on the time of day and the day of the week. Any administrator associated with this profile can only access FortiNAC as specified in the Login Availability field for the administrator profile.

1. Click **Users & Hosts > Administrators > Profiles**.
2. Click select an administrator profile and click **Modify**.
3. In the **Login Availability** field, select **Specify Time**.
4. In the **Time Range** section of the **Specify Time** dialog, enter the **From** and **To** times for the time of day that administrators should be able to access the network.
5. In the **Days of the Week** section, select the days during which these users should be allowed to access the network.
6. Click **OK**.

Manage guests tab settings

Field	Definition
Guest Account Access	You can give administrators with this profile privileges that allow them to manage all guest contractor accounts, regardless of who created them, only their own accounts, or no accounts. The privileges include whether the sponsors can add or modify accounts, locate guests or contractors, and view reports. No: Users can only see guest accounts they create and send credentials to those guests. Users cannot modify or delete any guest accounts. Own Accounts: Users can see guest accounts they create, send credentials to those guests, and modify or delete their own guest accounts. All Accounts: User can see all guest accounts in the database, send credentials to guests and modify or delete any guest accounts.

Field	Definition
Account Types	Individual: Sponsor can create single guest accounts. Within the constraints of the template, the sponsor may specify account start and end date. Each account has a unique name and password associated with it. Bulk: Sponsors may create multiple accounts with unique passwords by importing a bulk account file. Conference: Sponsors may create any number of conference accounts, or the number may be limited by a template. Conference accounts may be named identically but have a unique password for each attendee, have the same name and password, or have unique names and passwords.
Create Accounts Days in Advance (Maximum)	The maximum number of days in advance this sponsor is allowed to create accounts.
Create Accounts Active For Days (Maximum)	Determines the length of time the guest account remains active in the database.
Allowed Templates	Indicates whether the administrator can use all guest templates or only those in the Specify Templates > Selected Templates field. Default = All. Options include: • All Templates: Profile gives the administrator access to all templates in the database when creating guest accounts. • Specify Templates: Profile gives the administrator access to the templates listed in Selected Templates.
Specify Templates	Allows you to select guest/contractor templates available for administrators with this administrator profile. Use the arrows to place the templates needed in the Selected Templates column and the unwanted templates in the Available Templates column. If All Templates is selected in the Allowed Templates field, all templates are moved to the Selected Templates column and the arrows are hidden.
Available Templates	Shows the templates that have not been selected to be included in this administrator profile.
Selected Templates	Shows the templates selected to be included in this administrator profile.
Add Icon	Create a new guest/contractor template.
Modify Icon	Modify the selected guest/contractor template.

Profile devices tab settings

Field	Definition
Register, Delete, and Disable Profiled Devices	If enabled, the user can register, delete and disable devices that have been profiled by device profiler.
Modify Device Rule Confirmation Settings	If enabled, the user can change rule confirmation settings on devices that have been profiled by device profiler. Rule confirmation settings control whether or not device profiler checks a previously profiled device to determine if it still meets the criteria of the rule that categorized the device.

Field	Definition
Manage Profiled Devices Using These Rules	All Rules: includes current rules and any rules created in the future. Specify Rules: you must choose the rules from the Available Rules field and manually move them to the Specify Rules field.
Available Rules	Shows the existing rules you can select for this profile. Select the rule and click the right arrow to move it to the Selected Rules pane.
Selected Rules	Shows the rules you selected from the Available Rules section. The user can only access the devices associated with the rules in this list.
Add Icon	Create a new Device Profiling Rule. For information on rules, see Adding a rule on page 264 .
Modify Icon	Modify the selected Device Profiling Rule. For information on rules, see Adding a rule on page 264 .

Security events tab settings



The Security Events tab is only available when Security Incidents is enabled within your current license package.

Field	Definition
Allow Overriding of Recommended Actions	If enabled, the user can override the associated action when taking action on the alarm.
Allowed Actions for Security Events	All Actions: includes current actions and any actions created in the future. Specify Actions: you must choose the rules from the Available Actions field and manually move them to the Selected field.
Available Actions	Shows the existing actions you can select for this profile. Select the action and click the right arrow to move it to the Selected Actions pane.
Selected Actions	Shows the actions you selected from the Available Actions section. The user can only complete the actions in this list.

Modify administrator profiles

1. Click **Users & Hosts > Administrators > Profiles**.
2. A list of existing profiles is displayed.
3. Select a profile and click **Modify**. Refer to [Add an administrator profile on page 139](#) for settings.
4. Change the information and click **OK** to save.

If you modify an administrator profile, the changes apply to all administrators it is attached to, including those created before you modified the profile. Changes do not take effect until the associated administrators log out of FortiNAC and log in again.

The **Modify Admin Profile** window can also be accessed from the **Admin Users** view by clicking on the profile link associated with each administrator.

Delete an administrator profile

You can not delete an administrator profile if it is in use.

1. Click **Users & Hosts > Administrators > Profiles**.
2. Select an administrator profile and click **Delete**.
3. A message displays asking if you are sure. Click **Yes** to continue.

Copy an administrator profile

You can create a copy of an existing administrator profile and save it with a different name. This saves time when you create administrator profiles if you are only changing a few fields.

1. Click **Users & Hosts > Administrators > Profiles**.
2. The **Admin Profiles** option opens a window containing existing profiles.
3. To copy an administrator profile, select the profile and click **Copy**.
4. Modify information as needed.
5. Click **OK**.

Administrator profile mappings

Administrator profile mappings allow you to apply an administrator profile to an administrator when the user is added to an administrator group. An administrator profile mapping consists of an administrator profile that is linked to an administrator group.

Administrator profiles can be assigned to administrators based on the users' group membership. Administrator profile Mappings Policies are ranked in priority starting with number 1. When an administrator is added to an administrator group the group name is compared to the group in each administrator profile mapping starting with the first mapping (Rank 1) in the list. If the group does not match in the first mapping, the next one is checked until a match is found.

When groups are nested within a parent group, administrator profiles must be mapped to the groups that contain the users, and not the parent group only.

There may be more than one administrator group that is matched to this administrator; however, the first match found is the one that is used.

Administrator profile assignments are not permanent. The administrator is reevaluated each time that user is added to or deleted from an administrator group.

Settings

Field	Definition
Rank Buttons	Moves the selected mapping up or down in the list. Administrators are compared to administrator profile mappings in order by rank.

Field	Definition
Table columns	
Rank	Mapping's rank in the list of mappings. Rank controls the order in which administrators are compared to mappings.
Admin Profile	Name of the profile that is assigned when an administrator becomes a member of the associated group. See Administrator profiles on page 125 .
Group	Contains the required group for an administrator.
Last Modified By	User name of the last user to modify the mapping.
Last Modified Date	Date and time of the last modification to this mapping.
Right click options	
Copy	Copies the selected mapping.
Delete	Deletes the selected mapping.
Modify	Opens the Modify Mapping window for the selected mapping.
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746 .
 You must have permission to view the admin auditing log. See Add an administrator profile on page 139 .	

Mappings process

Administrator profile mappings establishes a profile for administrators who are members of a particular administrator group. Administrator profile mappings are ranked so that if an administrator is a member of more than one group, FortiNAC can determine which administrator profile should be applied to the user.

Example:

1. Administrator John is in Group A and Group B.
2. Group A is mapped to a guest sponsor profile and Ranked #5.
3. Group B is mapped to a Device Manager Profile and Ranked #2.
4. FortiNAC associates John with the Device Manager Profile because that mapping is higher in Rank and is the first match for John.



Adding an administrator to a group that has an administrator profile mapped can change the administrator profile applied to that user.

Administrator profiles are only applied to members of an administrator group when the administrator is added to the group or deleted from a higher ranking group. The administrator could be added to the group manually or on directory resynchronization. Review the scenarios below for information on the behavior of administrator profile mappings.

Administrator added to a group manually

- An existing administrator is added to administrator group A that is mapped to administrator profile C. The user is not in any other administrator groups. The administrator's profile is updated to profile C because it is mapped to group A.
- An existing administrator is added manually to administrator group A that is mapped to administrator profile C. The user is also in administrator groups B and C, but the new group A is ranked higher in the administrator profile mappings list and the new administrator profile C is assigned.

Administrator added to a group based on directory group membership

- Administrators are created automatically in FortiNAC when users authenticate to the directory and then access FortiNAC through the admin UI or by registering a host. The users are then assigned group membership according to their directory groups.

Possible scenarios that create administrators automatically are:

- If a user exists in the directory, for example jdoe, but the user is not a user of any kind in FortiNAC, when jdoe logs into the FortiNAC User Interface using a directory user id and password, a user "jdoe" is created in FortiNAC as an administrator.
- If a user exists in the directory, for example asmith, but the user is not a user of any kind in FortiNAC, when asmith registers a host via FortiNAC, a user for asmith, of type "user" is created. Then, when the directory Synchronization task runs, asmith becomes an administrator user in FortiNAC.
- If a user exists in the directory, for example tjones, but the user is not a user of any kind in FortiNAC, when tjones registers a host via FortiNAC, a user for tjones, of type "user" is created. If, before the directory Synchronization task runs, the user logs into the FortiNAC admin UI, the tjones user will transition to be an administrator at that time (i.e., not waiting for the directory sync.)
- When the directory synchronization is run, users are added to FortiNAC administrator groups that match the groups in the directory. Adding administrators to a group triggers an evaluation of administrator profile mappings. If the administrator is in multiple directory groups, the user will be assigned to multiple groups in FortiNAC, and the administrator profile will be assigned according to the administrator profile ranking.



When an administrator group is created in FortiNAC with the same name as a group being synchronized from a directory, the administrator group members will remain the same as the directory group members. Therefore, if you add a non-directory user to the administrator group and then synchronize the directory, the non-directory user is removed from the administrator group because the user is not a member of the directory group.

Modify ranks of administrator profile mappings

- The order of the administrator profile mapping records is changed modifying the ranking. A scheduled directory synchronization runs. Administrators' groups are updated each time the synchronization is run causing the administrator profile mappings to be analyzed again. Since the ranking has changed, some administrators that are members of more than one group are assigned different administrator profiles based on the new ranking.
- The order of the administrator profile mapping records is changed modifying the ranking. No directory is being used. Administrators continue to have the same administrator profiles because there is no mechanism to trigger a re-evaluation of group membership.

Administrator deleted from a group manually

- An existing administrator is deleted from administrator group A that is mapped to administrator profile C. The user is a member of Groups B and C mapped to Profiles D and F. A new profile is assigned based on one of the other groups used in the administrator profile mapping with the highest rank.
Administrator group B is mapped to administrator profile D. Administrator group C is mapped to administrator profile F. The mapping for Group B has the highest rank, therefore the administrator's profile is updated to administrator profile D.
- An existing administrator is deleted from Group A that is mapped to an administrator profile C. The user is not a member of any other group mapped to a profile. The user's administrator profile C is completely removed. The user loses his administrator status and becomes only a regular network user under **Users & Hosts > User Accounts**. To restore the user to an administrator you must add the administrator again with the same user ID and assign an administrator profile.

Administrator deleted from a group in the directory

- An existing administrator is deleted from administrator group A in the directory. The directory resynchronizes with FortiNAC which deletes the administrator from Group A that is mapped to administrator profile C. The user is a member of Groups B and C mapped to Profiles D and F. A new profile is assigned based on one of the other groups used in the administrator profile mapping with the highest rank.
Administrator group B is mapped to administrator profile D. Administrator group C is mapped to administrator profile F. The mapping for Group B has the highest rank, therefore the administrator's profile is updated to administrator profile D.
- An existing administrator is deleted from administrator group A in the directory. The directory resynchronizes with FortiNAC which deletes the administrator from Group A that is mapped to administrator profile C. The user is not a member of any other group mapped to a profile. The user's administrator profile C is completely removed. The user loses his administrator status and becomes only a regular network user under **Users & Hosts > User Accounts**. To restore the user to an administrator you must add the administrator again with the same user ID and assign an administrator profile.

Administrator group is deleted from FortiNAC

- An existing administrator is in group A that is mapped to administrator profile C. The user is not a member of any other group mapped to a profile. Group A is deleted from the groups view. The user's administrator profile C is completely removed. The user loses his administrator status and becomes only a regular network user under **Users & Hosts > User Accounts**. To restore the user to an administrator you must add the administrator again with the same user ID and assign an administrator profile.

Administrator profile mapping is deleted from FortiNAC

- Administrators are not affected when an administrator profile mapping is deleted from the data base until a user is added to or deleted from a Group. If the group is no longer mapped their profile is not updated. If the group continues to be mapped, their profile is updated as described in the previous scenarios.

When groups are nested within a parent group, administrator profiles must be mapped to the groups that contain the users, and not the parent group only.

Changing the ranking on existing administrator profile mapping records does not change profiles on administrators unless those users are in the directory and the directory is resynchronized.

Adding a new administrator profile mapping does not affect existing administrators until the directory is resynchronized or a user's membership in a mapped group changes.

If you are not using a directory, there is no mechanism for administrators to be reevaluated.

Add or modify a mapping

1. Click **Users & Hosts > Administrators > Profiles**.
2. Select **Admin Profile Mappings** from the menu.
3. Select an existing mapping and click **Modify** or click **Add**.
4. In the **Admin Profile** drop-down, select a profile. If the profile you need is not in the list, select **New** to create it. See [Add an administrator profile on page 139](#) for instructions.
5. In the **Group** drop-down, select an administrator group. If the group you need is not in the list, select **New** to create it. See [Add groups on page 845](#) for instructions.
6. Click **OK** to save.

Delete a mapping

Deleting an administrator profile mapping does not affect profiles assigned to administrators. They continue to have the same administrator profile until something triggers a re-evaluation such as a directory synchronization.

1. Click **Users & Hosts > Administrators > Profiles**.
2. Select **Admin Profile Mappings** from the menu.
3. Select an existing mapping and click **Delete**.
4. Confirm that you want to delete the mapping.

Limit access with groups

To control which hosts and ports administrators can access you can place those administrators in special groups. Then designate those special Admin groups to manage groups of hosts or ports.

Example:

Assume you have two administrators that are responsible for monitoring medical devices and nurses in a hospital. They should not see any other data. To accomplish this you must configure the following:

- Place the nurses' workstations into a host group.
- Place the medical devices to be monitored into a host group.
- Place the ports where the medical devices connect into a port group.
- Place these two administrators in a special administrator group.
- Assign these two administrator to a profile with permissions for **Manage Hosts & Ports**. Make sure the **Manage Hosts & Ports** setting on the **General** tab of the profile is set to **Restrict by Groups**.
- Set the administrator group to manage the nurses group, the medical device group and the port group.
- Remove these two administrators from the **All Management** group or they will have access to all hosts and ports.

When those administrators log into the admin UI, they can only see data associated with the nurses, medical devices or the ports in the groups they manage.

Make sure to remove affected administrators from the **All Management** group or they will continue to have access to all hosts and ports.

Administrators can still view all hosts and users from the Locate View if their administrator profile gives them permission for that view, but they can only modify those that are in the group they are managing.

1. Create the group of hosts or ports. See [Add groups on page 845](#) for instructions.
2. Create an administrator profile for with permissions for manage hosts & ports. Make sure the **Manage Hosts & Ports** setting on the **General Tab** of the profile is set to **Restrict by Groups**. See [Add an administrator profile on page 139](#)
3. Create an administrator group that contains the administrators responsible for the devices or ports.
4. Remove the administrators from the **All Management** group. See [Modify a group on page 846](#) for instructions.
5. Right-click on the administrator group and select **Manages**.
6. On the **Manages** window select the group(s) to be managed by marking them with a check mark.
7. Click **OK**.

Set privileges based on directory groups

To provide access to the FortiNAC user interface you can place administrators in special groups that set the appropriate privileges. Typically this is done for users in your directory, by placing them in special groups within the directory that correspond to matching groups in FortiNAC. When the directory is synchronized with FortiNAC, users in the appropriate groups will be given administrator privileges based on their group settings and the administrator profile mapping that matches the user's group.

The domain users group cannot be used to set administrator privileges because user details for users in that group are not populated in FortiNAC when a directory synchronization is done.

When an administrator group is created in FortiNAC with the same name as a group being synchronized from a directory, the administrator group members will remain the same as the directory group members. Therefore, if you add a non-directory user to the administrator group and then synchronize the directory, the non-directory user is removed from the administrator group because the user is not a member of the directory group.

Implementation

Directory

- Integrate your directory with FortiNAC. See [Directories on page 868](#) for configuration and integration information.
- Temporarily disable the directory synchronization task in the FortiNAC scheduler to prevent the synchronization from pulling directory information before the setup is complete. See [Scheduler on page 857](#).
- If you want to send e-mail to administrators, make sure to map the e-mail field in your directory to the e-mail field in FortiNAC. To set up this mapping go to **System > Settings > Authentication > LDAP**. Select the directory and click Modify. Select the **Attribute Mappings** tab and make sure that the e-mail field is configured. This setting allows users to receive e-mails based on device profiler settings, guest manager settings, and event to alarm mappings based on group membership.
- Create groups in the directory for each set of administrator privileges you wish to grant. For example, if you want to have administrators with full rights to FortiNAC and administrators who are just sponsors for guest access, create two groups in the directory, one for each type of administrator. Add the appropriate administrators to the new groups.
- Make sure the new groups are selected to be included when the directory and FortiNAC are synchronized. To select the groups go to **System > Settings > Authentication > LDAP**. Select the directory and click Modify. Click the Select groups tab and review the selected groups

FortiNAC

- All administrators require an administrator profile that provides permissions. Create the appropriate administrator profiles first. See [Administrator profiles on page 125](#).
- Go to the Groups View and create Administrator groups to contain the users who will be given access to FortiNAC. The group name must be absolutely identical to the name of the group in the directory.
- Since groups automatically brought over from the directory are typically Host groups, you must create the Administrator groups manually. If a group already exists with the name of one of the Administrator groups, you must delete that group and add it again as an Administrator group.
- Map administrator groups to administrator profiles. These mappings allow FortiNAC to determine the administrator profile that should be associated with an administrator based on the group that contains that user. Mappings are ranked and administrators are associated with the first mapping they match. See [Administrator profile mappings on page 144](#).

Example:

- Administrator John is in Group A and Group B.
- Group A is mapped to a guest sponsor profile and Ranked #5.
- Group B is mapped to a Device Manager Profile and Ranked #2.
- FortiNAC associates John with the Device Manager Profile because that mapping has a higher Rank and is the first match for John.
- Go to the Scheduler View in FortiNAC and enable the directory synchronization task. Run the task to update the groups. Users that have already registered in FortiNAC are updated immediately. New users that are not in the FortiNAC database but do exist in the directory are added to FortiNAC groups when they log into the admin UI the first time.
- Go to the groups view and verify that the correct users have been placed in each group. See [Groups on page 843](#).
- Go to the administrators view and verify that the administrator profile is correct for each user. See [Administrators on page 119](#).



If the root account for FortiNAC is placed in a group with an administrator profile other than the **System Administrator** profile, the administrator profile of this account will change. This could potentially leave you without a root or admin login that provides access to the entire FortiNAC product.



Aging for new administrators created by being added to a directory group is determined by Global Aging settings. See [Aging on page 1006](#) and [Aging out host or user records on page 241](#).

Add administrators to groups

You can add selected administrators to groups you have created. See [Groups on page 843](#) for detailed information on Groups and how they are used in FortiNAC.

1. Select **Users & Hosts > Administrators**.
2. Use the filters to locate the appropriate administrator(s).
3. Use Ctrl-click or Shift-click to select the records you wish to add to the group.
4. Click **Options** and select **Add Admin Users To Groups**.

5. The **Group Membership** view lists the available groups and sub-groups. Sub-groups are displayed under their parent group or groups.
6. To add the users to a group, click the box next to the group name and then click **OK**.
7. To create a missing group:
 - a. Click **Create Group**.
 - b. Enter a group name.
 - c. If the new group should be a sub-group of an existing group, enable the **Parent Group** option and select the appropriate group from the list.
 - d. **Description** is optional.
 - e. Click **OK** to save the new group.
8. Click **OK**.

Group membership

You can view or modify the group membership of an individual user.

1. Select **Users & Hosts > Administrators**.
2. Select the user, right-click and select **Group Membership**.
3. The **Group Membership** view lists the available administrator groups. A check next to a group name indicates that this user is contained in that group.
4. To add the user to a group, click the box next to the group name and then click **OK**.
5. To remove the user from a group, click to uncheck the box next to the group name and then click **OK**.

Configure secure mode

Secure SSL Mode can be used for administrator access. Unique security certificates for the appliances are required to use secure mode. Secure certificates in a high availability configuration may be used on both the primary and secondary appliances if the certificate provider licensing allows them to be transferred to their counterpart in the configuration.

FortiNAC appliances are pre-configured with a self-signed security certificate. The administrator logs in at the following URL, which provides secure access:

`https://<hostname_or_IP>:8443`

See [SSL certificates on page 509](#).

Guests & Contractors

Your enterprise may occasionally need to augment staff with contractors for short term projects. More often, you need to provide controlled network access for guests or remote attendees of conferences. Guest manager meets these demands by providing you with a set of tools to create limited network accounts for Guests and Contractors that are secure, role-based and provide access for a specified time period. Guest manager allows you to:

- Control the point of access for guests and contractors.
- Manage guest and contractor authorization.

- Ensure that guests and contractors receive the appropriate network resources for the amount of time the services are needed.
- Provide IT staff with control and tracking capabilities.
- Provide administrators that allow non-IT staff to create accounts and manage accounts for visiting users.

You must have a license for the guest manager feature. You must be sure to have enough concurrent licenses to provide a connection to the network for each guest. When a host connects to the network it uses one concurrent license. The license is released as soon as that host disconnects from the network. See [Licenses on page 29](#) for additional information.

When guests or contractors enter their temporary user name, password, and other required information, guest manager checks the credentials against the guest or contractor account. Guest manager denies access if the credentials do not match the entries in the guest manager database or LDAP directory, depending on which is being used for guest or contractor authentication. In addition, guests and contractors can be scanned to ensure that they have up-to-date antivirus software and pose no threat to the network.

Implementation

Guest manager is implemented at several levels. The initial setup is done by a FortiNAC administrator. Guest and contractor accounts are created and managed by an administrator called a sponsor. Finally, guests and contractors themselves follow a login process.

Administrators

Administrators have full rights to all parts of the FortiNAC system and can fully implement guest manager without needing a sponsor user to create accounts. However, in most organizations these responsibilities are divided up.

- Make sure that e-mail settings for your FortiNAC server have been configured. If they are not configured you will not be able to send email to guests with their account credentials.
- If you intend to use endpoint compliance policies and scan guest's and contractor's computers, set up the policies before creating templates.
- Each guest account that is created must be associated with a template that controls configuration details about that account, such as how long the account is valid or when the guest can access the network. Guest account types include guest, contractor, conference, and self registered guest. See [Guest & Contractor templates on page 164](#).
- Guest manager templates allow you to limit guest access to the network based on time of day or day of week. During the time that the guest is not allowed to access the network it is marked "At Risk" for the Guest No Access admin scan. If you choose to implement this feature for any template, the following requirements must be met:
 - You must have a quarantine or remediation VLAN on your network.
 - Under **System > Settings > Quarantine**, enable the quarantine VLAN option.
 - Ports through which a guest would connect must be in the Forced Remediation Group (applies only to wired ports).
 - The Model Configuration for all switches to which guests connect must have an entry for the quarantine VLAN. This applies to both wired and wireless switches and access points.
- Administrator profiles control what administrators can do when they are working in FortiNAC. If you intend to have an administrator create and manage guest accounts you must create an administrator profile to provide that user with the appropriate permissions. Sponsors profiles determine whether the sponsor can manage guest accounts, Kiosk Accounts, or self-registered guest accounts.

- Create any administrators or sponsors that will be responsible for creating and managing guests. Administrators can also be created and associated with an administrator profile automatically based on users and groups in your directory.
- To force guests and contractors to register and/or authenticate when they connect to the network, the ports to which they connect must be in a controlled access group such as Forced Registration.
- When guests or contractors connect to the network they are presented with a registration page. This page can be set up either by editing the existing registration pages directly (Portal V1) or using the portal configuration content editor (Portal V2).
- If you would like to provide guests with badges containing their login credentials, you must make sure the printer is set up correctly.
- If you would like to send guests their login credentials via an SMS message, enable any necessary Mobile Providers. See [Mobile providers on page 1](#). For guest account, enter **Self Registered Guest**. SMS messages are enabled by default and requires that you enable Mobile Providers.
- If you decide to use network access policy features of FortiNAC you must configure user/host profiles that correspond to guests. Then map a user/host profile to a network access configuration using a network access policy. See [Network access on page 482](#) for additional information.

Sponsors

Sponsors have the following responsibilities. Administrators can perform these functions also.

- When all of the preliminary setup steps have been completed, either the sponsor or the Administrator can create guest/contractor accounts.
- If self registration requests permission has been granted, sponsors can also approve or deny account requests for accounts from guests using the self registration feature.
- To facilitate your guests connection to the network you must give them information about their login credentials.
- If you are managing a large group of guests or contractors, you can use the Locate feature to find and manage guests. See [Locate hosts on page 276](#).

Sponsors with management permissions in their administrator profile can locate guests, contractors, registered hosts, and other sponsors.

Sponsors who are limited in their administrator profile to managing their own hosts, can not search for any other hosts. The **Sponsor** field in the **Locate** screen is automatically filled in with the sponsor's name and can not be changed.

Guest & Contractor users

Guest & Contractor > Users allows you to create and manage guest or contractor accounts. To initially set up the accounts, click **Add** and select a template set up by your administrator. Include the e-mail addresses of the guests or contractors as you create their accounts. You can then notify them of start times, required class materials, or other relevant information.

You may enter data specified as **Required** in the guest or contractor registration form, or you can let the guests and contractors enter the data themselves when they log into the portal. At that time, the required fields must be completed in order for the guest or contractor to log into the system.

Passwords are automatically generated when guest or contractor accounts are created. Generated passwords do not include characters that could be difficult to identify, including: the number one, the letter l (ell), the upper case letter I (eye), zero, upper or lowercase letter O. For conference accounts with shared passwords you have the option of creating your own password or generating one. FortiNAC does not recognize or restrict system-generated passwords that may be offensive.



Expected password display behavior

Passwords are only available to the Administrator during the UI login session where the Administrator creates the password.

Upon next login, however, the Administrator will no longer be able to view the password.

Once passwords are no longer visible, selecting the Print or Print Badge option within the user account will generate a new password. This makes the previous password null and void. The new password will be available to view/export/print during that UI login session.

Admin users are unable to view the passwords that conference users have created.

If you have account management privileges in your sponsor administrator profile, you may change or remove information in an account. Depending on your privileges, you may be allowed to manage all created accounts or only your own accounts.

Settings

Fields used in filters are also defined in this table.

Field	Definition
View Reports	Opens the Guest Accounts Report view. This option displays only when Guest/Contractor Accounts is accessed from the Users menu.
Table columns	
Enabled	Indicates guest account status. The account is either enabled (green check mark) or disabled (red x).
Sponsor	User name of the administrator or sponsor that created the guest account.
Type	Guest account type. Types include: • Guest: A visitor to your facility with limited or Internet-only network access. • Conference: A group of short- or long-term visitors to your organization who require identical but limited access to your network for typically one to five days. • Contractor: A temporary employee of your organization who may be granted all or limited network access for a specific time period generally defined in weeks or months.
Name	Guest's first and last name.
User	Guest's email account which is used as the user ID at login.
Starting Start Date	Date and time (using a 24-hour clock format) the account will become active for the guest or contractor.
Ending End Date	Date and time the account will expire.
Login Availability	Times during which the guest is permitted to access the network.
Role	Role is an attribute of a user or a host. It is used in user/host profiles as a filter when assigning network access policies, endpoint compliance policies, and Supplicant EasyConnect policies.

Field	Definition
Authentication	Indicates type of authentication used. Options include: Local and LDAP. Guests typically use Local authentication.
Security & Access Value	Attribute assigned to a guest that can be used as a filter. Common values are Guest, Contractor or Visitor.
Account Duration	There are two methods that work together for determining the length of time a guest account is active. The shortest duration of the two is the one that is used to remove a guest account from the database. • Account Duration (Hours): Option included in the guest template to limit the time a guest account created with this template remains in the database. If this is blank, the guest account end date is used. The Account Duration starts only when the guest user first logs in. For example, you could create a guest account with a date range that spans one week and if the account duration was 24 hours, they would be able to log in for one 24 hour period any time during that week • Account End Date: Option included on the Add Guest Account dialog to determine the date on which the guest account expires. This field is required when a guest account is created.
Reauth Period	Number of hours the guest or contractor can access the network before reauthentication is required.
Last Modified By	User name of the last user to modify the guest account.
Last Modified Date	Date and time of the last modification to this guest account.
Right click menu options	
Delete	To delete an account, select the account and click Delete . The account is deleted and will no longer show up in the created accounts window.
Modify	Change information in an existing guest or contractor account. This option also allows you to reset the information and reenter it. To modify an account select the account you want to change and click Modify. Conference accounts cannot be modified.
Reset Password	To reset an account password select the account and click Reset Password . The account password is automatically changed.
View	View additional account information such as passwords and guest or contractor phone numbers. Select an account and click View . This displays the Print, Send e-mail and Send SMS options for the selected account(s).
Send Email	Sends email to the selected guests containing their login information.
Send SMS	Sends a text message to the selected guests' mobile telephone containing their login information.
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746.

Field	Definition
	 You must have permission to view the admin auditing log. See Add an administrator profile on page 139 .
Select All	Selects all guest accounts displayed in the table.
Enable/Disable	Select the account and click Enable/Disable . The account status is changed. This is used to enable a guest account if a guest were to arrive earlier than expected.

Add Single Account

Administrators with sponsor administrator profiles can create and manage guest or contractor accounts. This helps to:

- Free IT staff from the daily burden of creating accounts for visiting users.
- Ensure that guest and contractor accounts get created ahead of time so they do not have to wait for their accounts to be created when they arrive.

To set up accounts for guests or contractors before they arrive at your organization:

1. Log into your sponsor account.
2. The **Guest/Contractor Accounts** window is displayed. Administrators select **Users & Hosts > Guests & Contractors > Users**.
3. Click **Add**.
4. Click **Single Account**.
5. Select a [Template](#). Enter the information. See **Settings** below for details.
6. Click **OK**. The View Accounts screen opens with the account information in it. See [Provide login information on page 164](#).
7. Click **Print** or **Send e-mail** or **Send SMS** to provide account information and password to the guest or contractor, or **Close**. These options are visible to you depending on the privileges you have in your profile. Additional text can be added to the printout or email by typing the text into the Notes tab on the guest/contractor template before creating the account. See [Create templates on page 167](#).

Guests also display on the user view. See [User accounts on page 194](#).

Settings

Field	Definition
Template	Click the down arrow on the Template box and select the type of template you want to use for the account.
Information required to create account	
E-mail	Enter the E-mail address of the guest or contractor. This is the only personal information you are required to enter.
Password	A password is automatically generated for this guest. Click Generate Password to generate a new password if necessary or enter a password manually. Password must meet the minimum length designated in the selected guest template.

Field	Definition
	 FortiNAC does not recognize or restrict system-generated passwords that may be offensive.
	 If LDAP is specified as the authentication method in the selected guest template, the Password field is not displayed.
Account Start Date	Click the calendar icon to the right to select a date or enter the date and time (using a 24-hour clock format) the account will become active for the guest or contractor.
Account End Date	Click the calendar icon to the right to select a date or enter the date and time (using a 24-hour clock format) the account will expire. At that time, the guest or contractor will no longer be able to access the network. This defaults to the date and time calculated based on the number of hours entered in the Account Duration field in the guest template. If this field is empty, no account duration has been entered in the guest template. Administrators that have an administrator profile with custom guest/contractor account permissions will be restricted to choosing an end date that is within the bounds of the "Create accounts active for days (maximum)" setting as defined in the administrator profile. For example, if your administrator profile has a "Create accounts active for days" set to 20, you will not be able to choose an end date that is more than 20 days ahead of the chosen start date. This date sets the user expiration date for the guest. The host registered to this guest inherits the setting for registered hosts in Global Aging. When the user expires, both the user and host are removed from the database. If the host expires first, then only the host is removed from the database. There are two methods that work together for determining the length of time a guest account is active. The shortest duration of the two is the one that is used to remove a guest account from the database. Account Duration (Hours): Option included in the guest template to limit the time a guest account created with this template remains in the database. If this is blank, the guest account end date is used. The Account Duration starts only when the guest user first logs in. For example, you could create a guest account with a date range that spans one week and if the account duration was 24 hours, they would be able to log in for one 24 hour period any time during that week Account End Date: Option included on the Add Guest Account dialog to determine the date on which the guest account expires. This field is required when a guest account is created.
Additional account information	

Field	Definition
First Name	The guest or contractor's required personal data and the fields below may be entered by the sponsor before the arrival of the guests, or may be left for the individual guests to fill out themselves.
Last Name	
Address	
City	
State	
Country	
Zip/Postal Code	
Phone	The Required Fields under the Additional Account Information heading are designated with an asterisk (*). These fields must be filled in before the guest or contractor will be granted network access.
Asset	
Reporting To	
Department	In this example, these fields were added when the template was created and marked as Required.

Add Bulk Accounts

Depending on permissions, as a guest manager sponsor you may be able to create and manage multiple guest or contractor accounts at one time. The process for creating bulk accounts is similar to that for creating single accounts.

1. Log into your sponsor account.
2. The **Guest/Contractor Accounts** window is displayed. Administrators select **Users & Hosts > Guests & Contractors > Users**.
3. Click **Add**.
4. In the **Add Account** screen, click **Bulk Accounts**.
5. Select a [Template](#).
6. Use the table below to fill in settings.

Field	Definition
Template	Choose either a Guest or Contractor Template.
Import Passwords	Enable this check box if you want to manually specify a password for each guest. the Password must be the last field in each record. If enabled you must specify a password for every guest account being imported. If the check box is disabled, FortiNAC generates a password for each guest account as it is imported.
 FortiNAC does not recognize or restrict system-generated passwords that may be offensive.	

Field	Definition
Account Information	You must create a separate record for each account you are creating. Type field place holders for data that you would like the guest to enter. Press Enter after each record to indicate that a new record has been started. You also have the option of importing from a text file. Required information for account creation. Use a comma to separate each field. You may choose to enter additional user information if it is available, but it is not required at this time. The guest or contractor will be prompted to fill in the missing fields before they can log into the network. If there is missing information, enter a comma in its place. If you intend to provide login credentials to guests via SMS messages sent to their mobile telephones, you must include mobile number and mobile provider name in the account list of fields. See Mobile providers on page 1 for instructions on accessing the list of names.
Import File From	If you have a CSV or text file of the user record information, click Import From File to import the text into the Account Information window. See Bulk guest import on page 159 for more information.
Account Start Date	The day the account becomes active. You can start the account only on one of the days defined in your profile.
Account End Date	The date the accounts become inactive. This date sets the User Expiration date for each Guest. A host registered to a guest inherits the setting for registered hosts in Global Aging. When the User expires, both the User and the Host are removed from the database. If the Host expires first, then only the Host is removed from the database.

- Click **OK**. The View Accounts screen opens with the account information in it. See [Provide login information on page 164](#).
- Click **Print** or **Send e-mail** or **Send SMS** to provide account information and password to the guest or contractor, or **Close**. These options are visible to you depending on the privileges you have in your profile. Additional text can be added to the printout or email by typing the text into the Notes tab on the guest/contractor template before creating the account. See [Create templates on page 167](#).

Guests also display on the user view. See [User accounts on page 194](#).

Bulk guest import

If you need to create many guest accounts simultaneously, you can create Conference accounts or Bulk accounts. Conference accounts are generated by the system and don't allow you to provide any additional guest information, thus preventing you from e-mailing credentials to attendees. Bulk accounts use data that you supply either by typing it into the Bulk Account screen or by importing it from a CSV or text file.

The fields used in the file vary depending on the template selected to create the accounts. When a guest account template is created you indicate the fields that will be required, optional or ignored for guests. E-mail address is the only field that is absolutely required for all guests and must be included in the file. Other fields, such as first name or last name, may be required but this does not mean that they have to be in the import file. It means that the guest cannot log onto the network unless this information is supplied, either by you in the import file or by the guest when they fill out a web form during the login process.

Using a CSV or text file

Requirements:

- Do not include a header row
- You must have a comma for each possible field
- You must have a carriage return at the end of each record.
- E-mail is mandatory because you must have a way to forward credentials to your guests
- If Import Passwords is enabled the password is mandatory and it must be the last field in the row of data
- If the template is set to send SMS messages to guests, you must include Mobile Number and Mobile Provider
- Other fields may be required for the guest to enter but are optional for the CSV file

1. Log into FortiNAC.
2. The **Guest/Contractor Accounts** window is displayed. Administrators select **Users & Hosts > Guests & Contractors > Users**.
3. Click **Add**.
4. In the **Add Account** screen, click **Bulk Accounts**.
5. Select the template that will be used to create these bulk accounts.
6. To manually enter passwords as part of the import file, enable **Import Passwords**. If you prefer that the system generate the passwords, disable this option. If Import Passwords is enabled, it is a required field for each guest. Without this data you cannot import the file.
7. Once the template has been selected you can see the fields that can be imported in a list across the screen. E-mail is bolded indicating that it is required for import. Fields that are preceded by an asterisk are required prior to login but are not necessarily required for import. Therefore, including them in your CSV or text file is optional. Note that if you intend to send login information to guests via SMS, Mobile Provider and Mobile Number fields must be included both in the template and in the import file.
8. For this example, assume that the list of fields on the Bulk Account window is as follows: **First Name, Last Name, Address, City, State, Zip, Email, Phone**
Based on the list of fields shown above, the CSV file could look like this:
Ana,Bahr,44 Bow St,Pittsfield,NH,03263,asbahr@yahoo.com,603-523-7676
,,,,,,jjones@yahoo.com,
James,Smith,,,,,,jsmith@aol.com,
9. Save the file as .csv or .txt and make note of its location on your hard drive.
10. On the Bulk Accounts window, click **Import From File**.
11. On the Import From File window, click **Choose File**. Browse to your CSV file, select it and click **Open**.
12. The contents of the file display in the Bulk Accounts window. Click **OK**.
13. The View Accounts screen opens with the account information in it. See [Provide login information on page 164](#).
14. Click **Print** or **Send e-mail** or **Send SMS** to provide account information and password to the guest or contractor, or **Close**. These options are visible to you depending on the privileges you have in your profile. Additional text can be added to the printout or email by typing the text into the Notes tab on the guest/contractor template before creating the account. See [Create templates on page 167](#).

Add Conference Accounts

As a sponsor, if you have been granted permission in your administrator profile, you may create Conference accounts, which are bulk accounts in which the account information may be the same for all attendees, or unique to each

conference attendee. Conference accounts ensure that attendees have the information they need to access the conference account ahead of time.

Before you create the conference account, determine how you want to manage attendee names and passwords. You may specify:

- Individual names and passwords
- The same name and password for all attendees (for example Seminar1, seminar123)
- Individual attendee names and the same password for all.

If you select Individual Passwords, they will be generated by guest manager. Generated passwords do not include characters that could be difficult to identify, including: the number one, the letter l (ell), the uppercase letter I (eye), zero, upper or lowercase letter O. In addition, the template used to create the Conference accounts may have specific characters to be excluded from passwords.

Create accounts

The only change that can be made to a conference account is to reset passwords. If you require additional changes, you must delete the accounts and create new ones.

1. Log into your sponsor account.
2. The **Guest/Contractor Accounts** window is displayed. Administrators select **Users & Hosts > Guests & Contractors > Users**.
3. Click **Add**.
4. On the Add Account screen click **Conference**.
5. Fill in the fields as needed.
6. Click **OK**. The View Accounts screen opens with the account information in it. See [Provide login information on page 164](#).
7. Click **Print** to print out account and password information, or **Close**. These options are visible to you depending on the privileges you have in your profile.

E-mail cannot be sent to these conference attendees unless you enter an e-mail address for each attendee to whom you would like to send e-mail using the **Modify User** option on the user view.

SMS messages cannot be sent to these conference attendees unless you enter a mobile number and mobile provider using the **Modify User** option on the user view.

Guests also display on the user view. See [User accounts on page 194](#).

Settings

Field	Definition
Template	Select a conference template.
Conference Type	The selection you make from the pull-down menu determines how user names and passwords are managed for the conference. If you click Generate Password, the Password is automatically populated. The length of the password is determined by the length requirement specified in the Conference template. The available options are: • Individual User Names/Individual Passwords: Individual passwords are generated for each attendee. Conference members are required to enter their

Field	Definition
	name and unique password. • Individual User Names/Shared Password: Enter a password in the Password field, or click Generate Password. Conference members are required to enter their name and the password that is shared among all conference attendees. • Shared User Name/Shared Passwords: Enter a password in the Password field, or click Generate Password. All conference attendees are required to enter the shared name and password.  FortiNAC does not recognize or restrict system-generated passwords that may be offensive.
Conference Name	Enter the name of the conference. Note that the name of the conference appears as the User Name (conference attendee name) in the list of attendees created when you click Apply on this window. This cannot be modified after the account is created. You must delete the account and create new conference accounts with a new name.
Password	Click Generate Password to generate a password or enter a password manually. Password must meet the minimum length designated in the selected Guest template. See the conference types listed above for additional details on generating Passwords.
Number of Attendees	Enter the maximum number of attendees who need network access.
Conference Start Date	Enter a date and time or click the Calendar icon.
Conference End Date	Enter date and time that attendees will no longer need network access. This defaults to the date and time calculated based on the number of hours entered in the Account Duration field in the template. For example, if the template Account Duration is set to 72 hours, the end date can be less than three days but it cannot be more than three days. If this field is empty, no Account Duration has been entered in the template and you can choose any end date. This date sets the User Expiration date for the Guest. A host registered to a guest inherits the setting for registered hosts in Global Aging. When the User expires, both the User and the Host are removed from the database. If the Host expires first, then only the Host is removed from the database. There are two methods that work together for determining the length of time a guest account is active. The shortest duration of the two is the one that is used to remove a guest account from the database. Account Duration (Hours): Option included in the guest template to limit the time a guest account created with this template remains in the database. If this is blank, the guest account end date is used. The Account Duration starts only when the guest user first logs in. For example, you could create a guest account with a date range that spans one week and if the account duration was 24 hours, they would be able to log in for one 24 hour period any time during that week

Field	Definition
	Account End Date: Option included on the Add Guest Account dialog to determine the date on which the guest account expires. This field is required when a guest account is created.

Accounts with sponsor privileges

As a guest manager sponsor, you must log into FortiNAC to create guest or contractor accounts. Once logged in, the permissions defined by your administrator in your sponsor's administrator profile are applied. Depending on the permissions, you could be presented with a **Locate** tab, a **Guest/Contractor Accounts** tab, a **View Reports** tab, or all three.



Visibility of account passwords is limited. See **Expected password display behavior** under [Guest & Contractor users](#).

Log in as a sponsor

You can access the sponsor privileges assigned to you only when you log into your account.

1. Use a web browser to access URL: `https://<Hostname>:8080`
2. Enter the username and password that was given to you by the administrator.
3. A screen with the end-user license agreement opens. To access your sponsor account, read the agreement and press **Accept**.
4. Based on your privileges, this screen will show a **Bookmarks** drop-down menu. From this menu you can select **Guest/Contractor Accounts** or **Locate** to locate hosts and users.

As a sponsor, you can:

- Create and manage Guest, Contractor, and Conference accounts.
- Locate guests, contractors, and other sponsors.
- Sign-in to the kiosk you are in charge of to allow guests to create their own accounts for network access.
Guest sponsor users who sign in to the kiosk to prepare it for arriving guests have very limited permissions. If you are responsible for both the kiosk and managing Guest, Contractor and Conference accounts, you will need to have separate logins for each responsibility.
- To search for host or user records, click the **Locate** tab to open the **Locate** screen. See [Locate hosts on page 276](#).
- As a sponsor you will typically want to create accounts for guest, contractors, and conference members before they arrive. To create and manage accounts, click **Bookmarks > Guest/Contractor** to open the **Create** screen. See [Guest or contractor accounts on page 1](#), [Add Bulk Accounts on page 158](#), or [Add Conference Accounts on page 160](#).
- To view reports of guest or contractor accounts and registrations, click the **View Reports** link at the top of the **Guest/Contractor Accounts** view.

In addition to these privileges, guest manager sponsor users may also have permission to manage a self-serve **kiosk** or to manage guest self registration. The kiosk allows guests to create their own accounts for network access. The guest self registration option allows guests to send a request for network access which can be approved or denied by the sponsor. A sponsor with permissions to manage a self-serve kiosk or guest self registration, does not have permission to

manage Guest, Contractor and Conference accounts. A user who is responsible for all of these types of guest account creation, must have a separate login for the Kiosk.

A kiosk is unique within guest manager. Once the sponsor's credentials for the kiosk have been entered, guests use the kiosk computer to create their own accounts. Network access is limited and there are generally time constraints. For more information on a self serve kiosk see [Using a kiosk on page 185](#).

Provide login information

After you have created a guest or contractor account, you may want to provide that user with his login information. This information can be printed, viewed on the screen, included in an e-mail or sent to a mobile phone via an SMS message.

To include additional text with the account information sent to the guest, you must add the text to the guest account template under the **Note** tab prior to creating the account. See [Create templates on page 167](#) for additional information.

Guests who use the self registration option in the portal receive their credentials automatically. You do not need to send account information to those guests unless they lose the information.

For information on printer settings for guest badges, see [Printer settings for guest badges on page 184](#).

1. Make sure you are on the **Guest/Contractor Accounts** view. Administrators select **Users & Hosts > Guests & Contractors > Users**.
2. The list of guest/contractor accounts is displayed.
3. Select one or more accounts for which you wish to view additional information.
4. Click **View**.
5. Do the following:
 - Click **Print** to print the guest/contractor account information on a full (8.5 X 11) page.
 - Click **Print Badge** to print out the badge containing the guest/contractor account information.
6. Click **Send Email** to send account information to the e-mail account listed.
7. Click **Send SMS** to send account information to the mobile phone number listed in the guest's account.
8. Click **Close** to close the window.

Guest & Contractor templates

As an administrator, you control guest, contractor, conference, and self registration accounts by creating templates for each account type. The templates include privileges you specify, such as account duration, and credential requirements. Each time a visitor account is created one of these templates must be applied.

The templates you define:

- Restrict or allow certain privileges for the sponsors who create guest, contractor, and conference accounts.
- Ensure that sponsors set up appropriate accounts for guests and contractors.
- Define the number of characters in the automatically generated passwords.
- Make sure data from the guest or contractor is provided to the sponsor.

You may grant sponsor privileges to an administrator who uses the templates to create and manage temporary guest and contractor accounts. Sponsors may also provide account details to guests by email, SMS message or printout. The entire process, from account creation to guest network access, is stored for audit and reporting.

From the **Guest/Contractor Templates** window you can add, delete, modify or copy templates.

Settings

Field	Definition
Name	Descriptive name for the template. Sponsors use this name when they select a template to create accounts.
Visitor Type	User type for the template. Corresponds to the account types of Guest and Contractor so that the correct view is presented to the user.
Role	Role is an attribute added to the user and the host. Roles can be used in user/host profiles as a filter. Note that these roles must first be configured in the Role Management view. If they are not configured, no role-based restrictions apply. Any additional roles you have configured are also listed here. The available default options are Contractor, Guest and NAC-Default. If you have not configured a Guest or Contractor role, any Host you register has the NAC-Default common role applied to it. See Visitor types on page 166 . For more on roles, see Roles on page 620 .
Authentication	Indicates type of authentication used for Guests or Contractors associated with this template. Options include: Local: User name and password credentials are stored in the local database.  For Conference accounts, authentication is Local only. LDAP: The email of the user is required, and is what guests and contractors use to log in. The email address maps to the created Guest user. When the email address is located in the LDAP directory, it is compared with the given password for the user. If it matches, the guest or contractor's credentials are accepted and they are granted access. RADIUS: Checks your RADIUS server for the email address (required) in the user's created account. If a match is found, it is compared with the given password for the user. If it matches, the guest or contractor's credentials are accepted and they are granted access.
Login Availability	Indicates when guests or contractors with this template can login to the network. Login Availability is within the timeframe you specify for the Account Duration. The available options are: • Always • Time range Guests created using this template are marked "At Risk" for the Guest No Access admin scan during the times they are not permitted to access the network.
Password Length	Required length of guest or contractor passwords. Must be between 5 and 64 characters.
Account Duration	There are two methods that work together for determining the length of time a guest account is active. The shortest duration of the two is the one that is used to remove a guest account from the database.

Field	Definition
	Account Duration (Hours): Option included in the guest template to limit the time a guest account created with this template remains in the database. If this is blank, the guest account end date is used. The Account Duration starts only when the guest user first logs in. For example, you could create a guest account with a date range that spans one week and if the account duration was 24 hours, they would be able to log in for one 24 hour period any time during that week Account End Date: Option included on the Add Guest Account dialog to determine the date on which the guest account expires. This field is required when a guest account is created.
Reauth Period (hours)	Number of hours the guest or contractor can access the network before reauthentication is required.
Security & Access Value	User specified text associated with guests created using this template that can be used as a filter. Used to assign a policy to a guest by filtering for this value.
Password Exclusions	List of characters that will not be included in generated passwords.
Last Modified By	User name of the last user to modify the template.
Last Modified Date	Date and time of the last modification to this template.
Right click menu options	
Export	Exports data to a file in the default downloads location. File types include CSV, Excel, PDF, or RTF. See Export data on page 116 .
Copy	Copy the selected Template to create a new record.
Delete	Deletes the selected Template. Accounts that were created with the template prior to deletion are still valid and retain the data that was in the template.
Modify	Opens the Modify Guest/Contractor Template window for the selected template.
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746 .
	 You must have permission to view the admin auditing log. See Add an administrator profile on page 139.
Used By	Display a list of users by administrator profile that are associated with the selected template. Click on a specific administrator profile to see the associated users. To select more than one profile use the Ctrl key.

Visitor types

Guest manager supports four basic types of accounts. They are identified on the Guest templates as Visitor types and are loosely defined as follows:

- **Guest:** A visitor to your facility with limited or Internet-only network access. For example, a guest might be on the premises for a one-day sales call or a three-day presentation. Any number of guest accounts may be created at one

time as bulk accounts. In this case, the email address is the same as the user name. Guests who need access for one day only may be managed by administrators with permission to manage guest self registration or self-serve kiosks. For more on Kiosks see [Using a kiosk on page 185](#).

- **Self-Registered Guest:** A visitor to your facility with limited or Internet-only network access who connects to your network on their own device to request a temporary account. The account request goes to a sponsor via e-mail. The sponsor can log into FortiNAC and approve or deny the request or, depending on your configuration, can approve or deny the request for the account directly from the e-mail. The account is created when the request is approved.
- **Conference:** A group of short- or long-term visitors to your organization who require identical but limited access to your network for typically one to five days. Conferences are often bulk accounts, in which attendees receive notification of the conference via, for example, email. Conference members may be given an identical generated user name and password that is specific to the conference: for example, *conference-1* or *training123*, individual passwords for individual attendees, or individual attendee names with a shared password. See [Add Conference Accounts on page 160](#). When the conference members register they enter their email address. Once they have registered, they fill in their name and other information.
- **Contractor:** A temporary employee of your organization who may be granted all or limited network access for a specific time period generally defined in weeks or months. Any number of contractor accounts may be created at one time as bulk accounts. In this case, the email address is the same as the user name.

Create templates

Use this option to create multiple templates for each of the Guest, Contractor, Conference and self-registered guest visitor types with a variety of permissions. Data fields allow you to collect data from your guests and store it in User Properties. If you are a FortiNAC administrator you have access to all templates and can assign any template of the correct type to any guest, contractor or conference user when you create their accounts. If you choose to create a sponsor user who is responsible for creating visitor accounts, the sponsor must be assigned a set of templates through the administrator profile. When the sponsor creates visitor accounts, he can only choose templates from the list you have assigned.

1. Click **Users & Hosts > Guests & Contractors > Templates**.
2. The Templates window appears. Click **Add**.
3. The **Add Guest/Contractor Template** window appears. Enter the information in the **Required Fields** tab as described in [Create templates on page 167](#).
4. Click the **Data Fields** tab to determine which fields will be required when a guest logs onto the network.
5. Click the **Note** tab to add a note to the printed access information to give the guest/contractor special login instructions or an SSID. See [Provide login information on page 164](#).
6. Click **OK** to create the template and add it to the list of templates.

Settings

All possible fields are included in this table. The fields shown on your screen will vary depending on the Visitor Type you select.

Field	Definition
Template Name	Type a descriptive name for the template. Sponsors use this name when they select a template to create accounts.
Visitor Type	User type for the template. Corresponds to the account types of Guest and Contractor so that the correct view is presented to the user. See Visitor types on page 166 .

Field	Definition
Use A Unique Role Based On This Template Name	Creates a role based on the template name and assigns that role to guests with accounts created using this template. Using the template name as a role allows you to limit network access based on the guest template by using the new role as a filter in a user/host profile. See User/host profiles on page 466. When using the Wireless Security feature to configure SSID mappings, the name of the guest template selected is used to create the appropriate user/host profile allowing you to limit SSID access based on guest template.
Select Role	Role is an attribute added to the user and the host. Roles can be used in user/host profiles as a filter. Note that these roles must first be configured in the Role Management view. If they are not configured, no role-based restrictions apply. Any additional roles you have configured are also listed here. The available default options are Contractor, Guest and NAC-Default. If you have not configured a Guest or Contractor role, any Host you register has the NAC-Default common role applied to it. See Visitor types on page 166. For more on Roles see Roles on page 620.
Security & Access Value	Enter a value, such as Guest or Visitor. This field is added to each guest user account that is created based on this template and can be used as a filter. When creating user/host profiles, you can filter for the contents of the Security & Access Value field to control which endpoint compliance policy is used to scan guest hosts.
Send Email	For Conference accounts, email cannot be sent until a guest has registered or you have modified the account via the User View > Modify option to enter an email address. Select this check box if you want a sponsor with this template to be able to send an e-mail confirmation to the guest's/contractor's email address. If not selected (default) guest or contractor credentials need to be printed or sent via SMS. For self-registered guest accounts this option is automatically checked and cannot be disabled.
Send SMS	For Guest or Contractor accounts, select this check box if you want a sponsor with this template to be able to send an SMS confirmation to the guest's/contractor's mobile phone. If not selected guest or contractor credentials need to be e-mailed or printed. For self-registered guest accounts this option is automatically checked and cannot be disabled. Requires that the guest or contractor provide both a mobile number and the mobile provider. These fields default to Required in the Data Fields tab.
Max Number Of Accounts	Only available when Visitor Type is set to Conference. Typically used when generating a large number of accounts for a conference. Limits the total number of accounts that can be created on the Conference Account window when this template is selected. To limit accounts, enable the check box and enter the maximum number of accounts that can ever be created using this template. For an unlimited number of accounts, leave the check box empty.
Password Length	Between 5 and 64 characters. Passwords that are automatically generated by guest manager contain at least one capital letter, one lower case letter, one alphanumeric character, and one symbol. If you have characters listed in Password Exclusions, those characters will not be used.

Field	Definition
	Note that for Conference accounts, once a template has been created, the sponsor may specify the individual different passwords for attendees when the sponsor creates the conference account. See Add Conference Accounts on page 160.  FortiNAC does not recognize or restrict system-generated passwords that may be offensive.
Password Exclusions	List of characters that will not be included in generated passwords.
Use Mobile Friendly Exclusions	Removes any existing entries and then populates the Password Exclusions field with a list of symbols that are typically difficult to enter on a mobile device. Modify the list of characters as needed. Characters include: !@#\$%^&*()_+~{} :"<>?-=[]\;',/
Reauthentication Period (hours)	Specify the number of hours the guest or contractor can access the network before reauthentication is required. To specify a reauthentication period you must first select the check box. Next fill in the reauthentication period in hours. If you do not select this check box, you will not have to specify a reauthentication period for guests or contractor accounts created with this template.
Authentication Method	Specify where authentication occurs: • Local: User name and password credentials are stored in the local database.  For Conference accounts, authentication is Local only. • LDAP: The email of the user is required, and is what guests and contractors use to log in. The email address maps to the created Guest user. When the email address is located in the LDAP directory, it is compared with the given password for the user. If it matches, the guest or contractor's credentials are accepted and they are granted access. • RADIUS: Checks your RADIUS server for the email address (required) in the user's created account. If a match is found, it is compared with the given password for the user. If it matches, the guest or contractor's credentials are accepted and they are granted access.
Account Duration	Select the check box to specify the duration of the account in hours. For all guests except those with shared conference accounts: The duration governs how long from creation the account remains in the database, regardless of the end date that is entered when creating the guest account. For shared conference accounts: The duration governs how long from guest Login the account remains in the database, regardless of the end date that is entered when creating the conference. For self-registered guest accounts this option is automatically checked and cannot be disabled. You must enter a duration.

Field	Definition
	There are two methods that work together for determining the length of time a guest account is active. The shortest duration of the two is the one that is used to remove a guest account from the database. • Account Duration (Hours): Option included in the guest template to limit the time a guest account created with this template remains in the database. If this is blank, the guest account end date is used. The Account Duration starts only when the guest user first logs in. For example, you could create a guest account with a date range that spans one week and if the account duration was 24 hours, they would be able to log in for one 24 hour period any time during that week • Account End Date: Option included on the Add Guest Account dialog to determine the date on which the guest account expires. This field is required when a guest account is created.
Propagate Hosts	Controls whether the Propagate Hosts setting is enabled or disabled on the user record for guest users created with this template. If enabled, the record for the host owned by the guest user is copied to all managed FortiNAC appliances. This field is only displayed if the FortiNAC server is managed by a FortiNAC Manager.
Login Availability	Select when guests or contractors with this template can login to the network. Login Availability is within the timeframe you specify for the Account Duration. The available options are: • Always • Specify Time: If you select this option, a window displays in which you specify the time range and select the days of the week. Click OK. Guests created using this template are marked "At Risk" for the Guest No Access admin scan during the times they are not permitted to access the network.
URL for Acceptable Use Policy	Optional. Directs the guest or contractor to the page you specify with the network policies when they login.
Resolve URL	Click to acquire the IP addresses for the URLs for Acceptable Use Policy and Successful Landing page. If the URL is not reachable, specify the IP address in the IP address field.
Portal version 1 settings	
URL for Successful Landing Page	Directs the guest or contractor to a certain page when they have successfully logged into the network and passed the scan in an endpoint compliance policy. This field is optional and is used only if you have Portal V1 enabled in portal configuration. If you are using the portal pages included with FortiNAC and controlled by the content editor in the portal configuration, this field is ignored.

Login availability time

This option allows you to limit network access for a guest or contractor based on the time of day and the day of the week. Any guest associated with a template, can only access the network as specified in the Login Availability field for the template.

If you set times for Login Availability, FortiNAC periodically checks the access time for each guest associated with the template. When the guest is not allowed to access the network the host associated with the guest is marked "At Risk" for

the Guest No Access admin scan. When the time is reached that the guest is allowed to access the network, the "At Risk" state is removed from the host. These changes in state occur on the guest host record whether the guest is connected to the network or not. If the guest host connects to the network outside its allowed timeframe, a web page is displayed with the following message: "Your network access has been disabled. You are outside of your allowed time window. To regain network access call the help desk."

Data fields

Specify which pieces of data will appear on the form the guest or contractor will be required to fill out in the captive portal. For self-registered guests this information is filled out with the request for an account. For Guests with an existing account, this information is filled out after they enter their user name and password on the login page. If the field has a corresponding database field, it is stored there and displayed on the **User Properties** window. If the field does not have a corresponding database field, it is stored and displayed in the Notes tab of the **User Properties** window and the **Host Properties** window. Hover over the field name to display a tool tip indicating where the data entered by the guest will be stored.

- **Required:** The data in this field must be entered in order for the guest or contractor to log in.
- **Optional:** Appears on the form, but is not required data from the guest or contractor.
- **Ignored:** Will not appear on the form.

The **E-mail** field is required. The fields listed below are default fields that are included with the original setup of guest manager. Field names can be modified by typing over the original name. Therefore, the fields on your template window may not match any of the fields in this list. If you rename a field, the data entered into that field by the guest is still stored in its original location. For example, if you modify the title of the Last Name field to say Mother's Maiden Name, the data is still stored in the Last Name field on the **User Properties** window.

Field	Definition
Last Name	Maximum length 50 characters. Stored in the Last Name field.
First Name	Maximum length 50 characters. Stored in the First Name field.
Address	Maximum length 50 characters. Stored in the Address field.
City	Maximum length 50 characters. Stored in the City field.
State (or Province/County)	Standard two-letter state abbreviation, or up to 50 characters. Stored in the State field.
Country	Maximum length 50 characters. Stored on the Notes tab.
Zip or Postal Code	Maximum length of 16. Stored in the Zip Code field.
Email	Email address of the guest or contractor. Stored in the E-mail field.
	 This field can be modified however FortiNAC expects the contents of the field to be an email address. This field tests for a valid email address and will not allow the user to proceed without one. If the label is something other than email and other types of data are entered, the guest account may not be able to be created.
Phone	Telephone number including international country codes (for example, +1, +44). Maximum length 16. Stored in the Phone field.

Field	Definition
Mobile Phone	Mobile Telephone number. Maximum length 16. Stored in the Add/Modify User window.
Mobile Provider	The name of the company that provides the guest with Mobile service. The guest is provided with a list of possible providers. Stored in the Add/Modify User window.
Asset	Text field for computer serial numbers, manufacturer's name and model number, or any other asset identifier of the guest's or contractor's computing platform. Stored in the Serial Number field. Max.length 80 characters.
Reason	The reason for the guest's or contractor's visit. Max. length 80 characters. Stored on the Notes tab.
Person Visiting	Maximum length 50 characters. Stored on the Notes tab.
Buttons	
Add Field	Click to add new data fields to track additional guest or contractor data, such as license plate numbers or demo equipment details. Maximum length 80 characters. Type the name of the field in the pop-up window. Select whether to make the field required or optional. Once new fields have been added they are stored in the Notes tab of the user's account. To see these fields go to the User Properties window.
Delete Field	Delete a data field from the list. Only those fields that have been created by an administrator can be deleted. System fields can be set to Ignore so they do not display, but cannot be deleted from the template.
Reorder Fields	Changes the order of the fields as they appear in the Guest or Contractor Form. Click this button to reorder account information fields. In the pop-up window, click Move Up or Move Down and OK.

Notes

The Notes tab on the template creation window allows you to provide additional information to guests and contractors. After you have created a Guest or Contractor account, you may want to provide that user with his login information. Login information can be printed, viewed on the screen, sent via text message to a mobile telephone or included in an amalgamate text added on the Notes tab is appended to the guest information included in the printout, email or text message. See [Provide login information on page 164](#) for additional information.

Endpoint compliance policies for guests

Endpoint compliance policies and the agents that run associated scans are assigned based on the rules contained within the Policy. FortiNAC selects a scan and an agent by comparing guest and host data to the user/host profile in each policy beginning with the policy ranked number 1 until a match is found. When a match is found the scan and agent are assigned and the guest's computer is scanned. If you want to create a specific policy for guests, you must define a policy that searches for user data that only guests will match and place it at the beginning of the list of policies.

Example 1

In this example the policy will apply to guests based on their Role. Create a policy that has the following settings:

User/host profile

- **Where:** Leave this field blank.
- **Who/What by Group:** Leave this field blank.
- **Who/What by Attribute:** Add a filter for users. Within the filter enable Role and enter the name of the Role assigned to guests. Typically the Role is named Guest, but you may have chosen to use a different role for Guests. Roles are assigned by the guest template used to create the guest account.
- **When:** Set to Always.

Scan

- **Scan:** Create a scan to evaluate guest computers for compliance.

Endpoint compliance configuration

- **Scan:** Select the scan you wish to apply to guests.
- **Agent Tab:** Select the agent that should be used.

Endpoint compliance policy

- **User/Host Profile:** Select the profile that determines who is assigned this policy.
- **Endpoint Compliance Configuration:** Select the configuration that determines the scan and agent used.

Example 2

In this example the policy will apply to guests based on their Security & Access Value. Create a policy that has the following settings:

User/host profile

- **Where:** Leave this field blank.
- **Who/What by Group:** Leave this field blank.
- **Who/What by Attribute:** Add a filter for users. Within the filter enable Security & Access Value and enter the name of the Security & Access Value assigned to guests. These values are assigned by the guest template used to create the guest account.
- **When :** Set to Always.

Scan

- **Scan:** Create a scan to evaluate guest computers for compliance.

Endpoint compliance configuration

- **Scan:** Select the scan you wish to apply to guests.
- **Agent Tab:** Select the agent that should be used.

Endpoint compliance policy

- **User/Host Profile:** Select the profile that determines who is assigned this policy.
- **Endpoint Compliance Configuration:** Select the configuration that determines the scan and agent used.

Modify templates

1. Click **Users & Hosts > Guests & Contractors > Templates**.
2. The Guest/Contractor Template Management window opens with a list of created templates.
3. Select the template and click **Modify**. Change the name of the template, or other information and parameters.



Once the template has been modified the modifications will only apply to new accounts created from the template. All old accounts made from the template remain the same.

4. Click **OK**.

Copy templates

You may copy a template, save it under another name, and use it as the basis for a new template.

1. Click **Users & Hosts > Guests & Contractors > Templates**.
2. The Guest/Contractor Template Management window opens with a list of created templates.
3. Select the template and click **Copy**.
4. Change the name of the template, or other information and parameters.
5. Click **OK**.

Delete templates

You may delete a template at any time. Accounts that were created with the template prior to deletion are still valid and retain the data that was in the template.

1. Click **Users & Hosts > Guests & Contractors > Templates**.
2. The **Guest/Contractor Template Management** window opens with a list of created templates.
3. Select the template and click **Delete**.
4. A confirmation message is displayed. Click **Yes** to delete the template.

Administrator profile

In FortiNAC, you can create an administrator and give that user an administrator profile that contains special permissions for the Guest/Contractor feature set. These privileges are designed to restrict this user to certain parts of the program. See [Administrator profiles on page 125](#).

For guest manager, this type of user is referred to as a sponsor in documentation because that person sponsors incoming guests and contractors. Creating a sponsor administrator profile allows the user to manage guest, contractor,

conference or self-registered guest accounts. For more information on the types of accounts, see [Visitor types on page 166](#).

Guest manager supports multiple UPN formats (for example, @gcs.xyztech.com) so sponsors do not have to type their full user login name. As administrators create guest or contractor accounts, their user name is added as a part of the guest or contractor record for reporting purposes.

Additional permissions can be given to sponsors based on the parameters of their responsibilities. Create one or more administrator profiles for these types of users. Sponsor administrator profiles determine whether the sponsor can manage guest accounts, Kiosk Accounts, or self-registered guest accounts.

Add a guest manager profile

This procedure describes how to create a specific administrator profile for an administrator with permissions for guest manager. As a sponsor, the administrator can create guest or contractor accounts. For details on all of the options that can be include in an administrator profile, see [Add an administrator profile on page 139](#).

If an administrator profile has Kiosk Mode enabled, the corresponding user can only log into the Kiosk computer to make it available to arriving guests. That user cannot create accounts. You may need to create a sponsor who can manage accounts and a second sponsor to use for the self-service Kiosk. See [Add a guest kiosk profile on page 177](#).

To create an administrator profile you must first be logged into your Administrator account. Follow the steps below to add an administrator profile for an administrator that is considered a sponsor for incoming guests:

1. Click **Users & Hosts > Administrators > Profiles**.
2. Click **Add**. The **Add Admin Profile** screen appears with the **General** tab highlighted.
3. On the **General** tab, enter a name for the profile, such as **Guest Sponsor**.
4. Under **Manage Hosts and Ports** select **All**.
5. Leave the defaults for the remaining fields and click on the **Permissions** tab.
6. On the **Permissions** tab note that some permissions are dependent on each other. Refer to the [Permissions list on page 133](#) for additional information.
7. The minimum that this sponsor must have is the **Guest/Contractor Accounts** permission set. Select all of the check boxes for this set including the **Custom** check box.
8. When you select the Guest/Contractor permission set, the **Landing Page** field defaults to **Guest/Contractor Accounts**.
9. In addition you may want include self registration requests, which allow a sponsor to Allow or Deny guest access to a user who has registered through the captive portal. This is not required.
10. The **Manage Guests** tab is enabled when Custom is selected for the guest/contractor accounts permission set. Click on the **Manage Guests** tab.
11. Use the table below to configure the settings.

Field	Definition
Guest Account Access	You can give administrators with this profile privileges that allow them to manage all guest contractor accounts, regardless of who created them, only their own accounts, or no accounts. The privileges include whether the sponsors can add or modify accounts, locate guests or contractors, and view reports. No: Users can only see guest accounts they create and send credentials to those guests. Users cannot modify or delete any guest accounts.

Field	Definition
	Own Accounts: Users can see guest accounts they create, send credentials to those guests, and modify or delete their own guest accounts. All Accounts: User can see all guest accounts in the database, send credentials to guests and modify or delete any guest accounts.
Account Types	Individual: Sponsor can create single guest accounts. Within the constraints of the template, the sponsor may specify account start and end date. Each account has a unique name and password associated with it. Bulk: Sponsors may create multiple accounts with unique passwords by importing a bulk account file. Conference: Sponsors may create any number of conference accounts, or the number may be limited by a template. Conference accounts may be named identically but have a unique password for each attendee, have the same name and password, or have unique names and passwords.
Create Accounts Days in Advance (Maximum)	The maximum number of days in advance this sponsor is allowed to create accounts.
Create Accounts Active For Days (Maximum)	Determines the length of time the guest account remains active in the database. There are two methods that work together for determining the length of time a guest account is active. The shortest duration of the two is the one that is used to remove a guest account from the database. Account Duration (Hours): Option included in the guest template to limit the time a guest account created with this template remains in the database. If this is blank, the guest account end date is used. The Account Duration starts only when the guest user first logs in. For example, you could create a guest account with a date range that spans one week and if the account duration was 24 hours, they would be able to log in for one 24 hour period any time during that week Account End Date: Option included on the Add Guest Account dialog to determine the date on which the guest account expires. This field is required when a guest account is created.
Can View Passwords	Enabled by default. Controls whether or not passwords generated for guest accounts are displayed to the operator that created the account. If disabled, the operator cannot view the password. Only random passwords are generated. Guests can still be informed of their password using email or SMS, depending upon template settings. See Create templates on page 167 .
Allowed Templates	Indicates whether the administrator can use all guest templates or only those in the Specify Templates > Selected Templates field. Default = All. Options include: All Templates: Profile gives the administrator access to all templates in the database when creating guest accounts. Specify Templates: Profile gives the administrator access to the templates listed in Selected Templates.

Field	Definition
Specify Templates	Allows you to select guest/contractor templates available for administrators with this administrator profile. Use the arrows to place the templates needed in the Selected Templates column and the unwanted templates in the Available Templates column. If All Templates is selected in the Allowed Templates field, all templates are moved to the Selected Templates column and the arrows are hidden.
Available Templates	Shows the templates that have not been selected to be included in this administrator profile.
Selected Templates	Shows the templates selected to be included in this administrator profile.
Add Icon	Create a new guest/contractor template. For information on templates, see Create templates on page 167 .
Modify Icon	Modify the selected guest/contractor template. For information on templates, see Create templates on page 167 .

12. Click **OK** to save.

Add a guest kiosk profile

A kiosk allows visitors to your facility to create their own account. Guests have a maximum of 24 hours of access to your network, which may be only during certain hours of the day, or a pre-defined number of hours from when they log on. Guests may simply be queried for pre-defined contact data. In any case, at 11:59 PM each day, or after the allowed number of hours has elapsed, kiosk guest accounts expire.

All other profile options are disabled if kiosk mode is enabled, because guests creating their own accounts would not need access to other options.

For added security, sponsors should use a kiosk browser. Kiosk browsers block users from accessing other programs on the host or other web sites.

This procedure describes how to create a profile that gives a sponsor permission to manage a kiosk. A sponsor with kiosk mode enabled cannot access any of the regular FortiNAC windows. That user can log in to display the guest login web page and make it available on the kiosk PC.

To create a profile you must first be logged into your Administrator account.

1. Click **Users & Hosts > Administrators > Profiles**.
2. Click **Add**. The **Add Admin Profile** screen appears with the **General** tab highlighted.
3. On the **General** tab, enter a name for the profile, such as kiosk sponsor.
4. Use the table below to fill out the settings.
5. Under **Manage Hosts and Ports** select **All**.
6. Select **Enable Guest Kiosk**.
7. In the **Kiosk Template** field select a guest/contractor account template. All guest accounts created through the Kiosk will use this template.
8. In the **Kiosk Welcome Text** field type the message that a guest will see when they create a guest account through the Kiosk.
9. Click **OK** to save.

Settings

Field	Definition
Name	Enter a name that describes the profile, such as kiosk sponsor.
Logout After	User is logged out after this amount of time has elapsed without any activity in the user interface.
Login Availability	Specify when this sponsor can log into the network: • Always • Specify Time The Specify Time option requires you to specify an hourly time range and the days of the week the sponsor can log in.
Manage Hosts And Ports	Restricts an administrator to a specific set of hosts or ports. The set is defined by host and port groups that are assigned to be managed by a specific group of administrators. Any administrator that has a profile with this option enabled can only view and or modify a subset of the data in FortiNAC. Typically, this type of user would ONLY have the Manage Hosts & Ports permission set on the Permissions tab, therefore, this setting is not used frequently. Default = All. • All: All groups containing hosts and ports can be accessed. • Restrict By Groups: Enables the restriction of administrator • s to specific hosts and ports. For an overview and additional setup information, see Limit access with groups on page 148 .
Note	User specified note field. This field may contain notes regarding the data conversion from a previous version of FortiNAC for an existing administrator profile record.
Enable Guest Kiosk	If you enable this mode, sponsors can log into FortiNAC to provide visitors self-serve account creation through a kiosk. For added security, use a kiosk browser. See Using a kiosk on page 185 to read the sponsor's procedure. Sponsors with this profile cannot do anything except log into the Kiosk PC to display the Guest Login page. Sponsors who need to manually create visitor accounts cannot have Kiosk mode enabled.
Kiosk Template	Select a Kiosk template for this sponsor. All visitors who use the self-service Kiosk when this sponsor is logged in will be assigned this template.
Kiosk Welcome Message	Enter the message that will appear when the kiosk user creates a guest account.

Add a guest self registration profile

Guest self registration allows visitors to request a temporary or guest account from their own device. A sponsor receives an email indicating that a request has been received from a guest. The sponsor responds to the request by approving or denying it. Sponsors with the guest self registration profile or with a guest manager profile and administrators can respond to a self registration request from a guest.

Anyone in your organization can be a sponsor for guest self registration. They must be entered into FortiNAC as an administrator and that user account must have a guest self registration administrator profile applied. You can quickly create sponsors by using directory groups. See [Set privileges based on directory groups on page 149](#).

Guests can access your network for the length of time specified by the account duration. Availability can be 24 hours a day or limited to specific hours during the day.

To create a profile you must first be logged into your administrator account.

1. Click **Users & Hosts > Administrators > Profiles**.
2. Click **Add**. The **Add Admin Profile** screen appears with the **General** tab highlighted.
3. On the **General** tab, enter a **Name** for the profile.
4. Use the table below for details on the fields in the General Tab.
5. Under **Manage Hosts and Ports** select **All**.
6. Leave the defaults for the remaining fields and click on the **Permissions** tab.
7. On the **Permissions** tab note that some permissions are dependent on each other. Refer to the [Permissions list on page 133](#) for additional information.
8. The minimum that this sponsor must have is the **Self Registration Requests** permission set. Select all of the check boxes for this set.
9. When you select the **Self Registration Requests** permission set, the **Landing Page** field defaults to **Self Registration Requests**.
10. Click **OK**.

Settings

Field	Definition
Name	Enter a name that describes the profile, such as kiosk sponsor.
Logout After	User is logged out after this amount of time has elapsed without any activity in the user interface.
Login Availability	Specify when this sponsor can log into the network: • Always • Specify Time The Specify Time option requires you to specify an hourly time range and the days of the week the sponsor can log in.
Manage Hosts And Ports	Restricts an administrator to a specific set of hosts or ports. The set is defined by host and port groups that are assigned to be managed by a specific group of administrators. Any administrator that has a profile with this option enabled can only view and or modify a subset of the data in FortiNAC. Typically, this type of user would ONLY have the Manage Hosts & Ports permission set on the Permissions tab, therefore, this setting is not used frequently. Default = All. • All: All groups containing hosts and ports can be accessed. • Restrict By Groups: Enables the restriction of administrators to specific hosts and ports. For an overview and additional setup information, see Limit access with groups on page 148 .

Field	Definition
Note	User specified note field. This field may contain notes regarding the data conversion from a previous version of FortiNAC for an existing administrator profile record.
Enable Guest Kiosk	Do not enable this field for the Self Registered Guest administrator profile. If you enable this mode, sponsors can log into FortiNAC to provide visitors self-serve account creation through a kiosk. For added security, use a kiosk browser. See Using a kiosk on page 185 to read the sponsor's procedure. Sponsors with this profile cannot do anything except log into the Kiosk PC to display the Guest Login page. Sponsors who need to manually create visitor accounts cannot have Kiosk mode enabled.

Administrators

When you create or modify an administrator, you must attach an administrator profile to the account. Before adding administrators to manage guests, create an administrator profile that contains the set of permissions that allow the administrator to sponsor guest, contractor, or conference accounts. The profile limits the administrator's access to FortiNAC features.

When an administrator with an administrator profile logs into FortiNAC, the system presents the views available based on the user's default permissions. You can configure administrators to authenticate locally or externally via RADIUS or LDAP. If the administrator cannot be authenticated, an error message specifying the problem displays.

Add an administrator

If you are creating administrators to manage guests or devices, you must create an administrator who has the appropriate administrator profile associated. See [Administrator profiles on page 125](#).

1. Select **Users & Hosts > Administrators**.
2. Select **Add**.
3. Enter an alphanumeric **User ID** for the new administrator and click **OK**.
 As you enter the user ID, the network user database is checked to see if there is a current user with the same ID and a drop-down list of matching users is displayed.
 If you enter an ID that already exists as a regular network user, the network user and the administrator become the same person with a single account. This allows you to give a network user administrator privileges to help with some administrative tasks.
4. Use the table of below for settings:

Field	Definition
Authentication Type	Authentication method used for this administrator. Types include: • Local: Validates the user to a database on the local FortiNAC appliance. • LDAP: Validates the user to a directory database. FortiNAC uses the LDAP protocol to communicate to an organization's directory. • RADIUS: Validates the user to a RADIUS server.

Field	Definition
Admin Profile	Profiles control permissions for administrators. See Administrator profiles on page 125. • Add: Opens the administrator profiles window allowing you to create a new profile without exiting the Add User window. • Modify: Allows you to modify the selected administrator profile. Note that modifications to the profile affect all administrators that have been assigned that profile.
User ID	Unique alphanumeric ID for this user.
Password	Password used for local authentication. If you authenticate users through LDAP or RADIUS, the password field is disabled and the user must log in with his LDAP or RADIUS password.
First Name	User's first name.
Last Name	User's last name.
Address	Optional demographic information.
City	
State	
Zip/Postal Code	
Phone	
E-mail	E-mail address used to send system notifications associated with features such as alarms or profiled devices. Also used to send guest self registration requests from guests requesting an account. For multiple e-mail addresses, enter addresses separated by commas or semi-colons. Messages are sent to all e-mail addresses provided.
Title	User's title, such as Mr. or Ms.
Mobile Number	Mobile Phone number used for sending SMS messages to administrators.
Mobile Provider	Mobile provider for the mobile phone number entered in the previous field. Used to send SMS messages to administrators. This field also displays the format of the SMS address that will be used to send the message. For example, if the provider is US Cellular, the format is xxxxxxxxx@email.uscc.net, where the x's represent the user's mobile phone number. The number is followed by the email domain of the provider's message server.
Notes	Free form notes field for additional information.
User Never Expires	If enabled, administrators are never aged out of the database. The default is enabled.  Administrators assigned the System Administrator profile cannot be aged out.

Field	Definition
Propagate Hosts	The Propagate Hosts setting controls whether or not the record for the host owned by the user is copied to all managed FortiNAC appliances. This field is only displayed if the FortiNAC server is managed by a FortiNAC Control Manager.

- Click **OK** to save the new user.

Portal page setup

If you are using the portal pages distributed with FortiNAC you may need or want to edit some of the settings that apply to guest users. Below is a list of settings that should be edited for guests. For a description of each field and how to use it, hover over the field in the portal content editor.

The portal content editor is arranged in a tree configuration. As you select an item on the left, the pane on the right displays corresponding options or settings that can be edited to manipulate how guests are treated in the portal and what is displayed on the web pages used by guests.

Options marked with an asterisk are not limited to being used for guest. These options may be displayed on many portal pages. For example, the instructions page can be enabled as a link on the guest registration page and the user registration page.

Tree Option	Settings
Registration > Login Menu Authentication > Login Menu	• Guest Login Enabled • Guest Login Title • Guest Login Link • Guest Login Order
Registration > Login Menu	• Self Registration Guest • Self Registration Guest Login Title • Self Registration Guest Login Link • Anonymous Authentication Enabled • Anonymous Authentication Title • Anonymous Authentication Link • Anonymous Authentication Order
Registration > Self Registration Login	• Window Title • Left Column Content • Request Page Title • Request Page Introduction • Request Page Form Title • Request Access Button Text • Pending Page Title • Default Sponsor Email • Sponsor Email Label • Notify Sponsor of Guest Details • Accept Notification • Login Username Label • Login Password Label

Tree Option	Settings
	• Require Sponsor Approval • Guest Request Expiration (minutes) • Request Pending Message • Deny Notification • Expired Notification • Cancel Request Button Text • Message from Sponsor Header • Sponsor Email Intro Text • Sponsor Approval Link Requires Login • Sponsor Email Login Link Text • Sponsor Email Approve Link Text • Sponsor Email Deny Link Text • Notify User via Portal Page • Show Password in Portal Page Notification • Notify User via Email • Notify User via SMS • Default Guest Template • Acceptable Use Policy • Acceptable Use Policy Checkbox Text • URL for Acceptable Use Policy • Link text for Acceptable Use Policy URL • Text for Acceptable Use Policy • Instructions
Registration > Primary Guest Login Authentication > Primary Guest Login	• Window Title • Title • Left Column Content • Introduction • Form Title • User Name Label • Password Label • Missing Fields • Instructions
Registration > Secondary Guest Login Authentication > Secondary Guest Login	• Window Title • Title • Left Column Content • Main Content • Introductory Paragraph • Form Button Text • Account Expiration Label • Login Availability Label
*Registration > Instructions	• Window Title • Title • Left Column Content

Tree Option	Settings
*Authentication > Instructions	• Introduction • Show Windows Instructions • Windows Instructions • Show macOS Instructions • macOS Instructions • Show Linux Instructions • Linux Instructions • Show Other Instructions • Other Instructions Title • Other Instructions • Display as Accordion View
*Registration > Success *Authentication > Success	• Window Title • Title • Left Column Content • Progress Bar Enabled • Progress Bar Title • Please Wait message • Success Message • Finished Message

Printer settings for guest badges



Visibility of account passwords is limited. See **Expected password display behavior** under [Guest & Contractor users](#).

In guest manager, administrators you designate as sponsors can access guests' account credentials that show the user name, password, and access start time and end time. Sponsors may print the account details, e-mail them or send them via an SMS message directly to guests after account creation.

If sponsors managing guest kiosks or conferences need to print badges, contact your IT Manager to assure that printer settings are optimized for badge creation:

Make sure the label printer is the default printer for kiosks.

- In the Printer Properties, Paper Options settings, set the paper label size to a minimum of 2" x 2-3/4" (5.1 cm x 7 cm).
- In the Page Handling Settings, make sure that Auto-Rotate is enabled to automatically adjust the orientation to fit the label's orientation on the sheet.
- Test to make sure that text is centered and fits on each label.

Events and alarms

Certain actions within guest manager generate events that appear in the Event Log. Examples of guest manager events are listed in the following table.

Event	Definition
Conference Created	Using guest/contractor accounts you can create a batch of conference user accounts. This event is generated when those accounts are created and indicates the number of accounts created.
Guest Account Created	New guest account is created.
Guest Account Deleted	Guest account is deleted.

If certain event conditions occur, you are immediately informed of the condition through the alarm notification system. You can define and map additional events to alarms.

For more information on events and alarms, e-mail notifications, and how to map events to alarms see [Map events to alarms on page 784](#).

Guest/contractor login

The portal defaults to a guest or contractor login link which opens the default guest authentication page. To log into the network, guests and contractors must enter the required data fields on their account.

1. From the Guest or Contractor Login page, the guest clicks the **Start** link to open the Welcome screen.
2. Guests enter the Username and the Password that was provided to them by a printout, e-mail or SMS message.
3. Guests click **Download** or **Register** to open the Registration screen.
4. The fields that appear in the Registration screen are those that were defined in the guest/contractor template. Fields with an asterisk indicate to the guest that this information must be entered in order to register.
5. The guest clicks **Acceptable Use Policy** to read, accept, and exit the Acceptable Use Policy page.
6. The guest clicks **Continue**. If the host passes the endpoint compliance policy requirements, the successful landing page is displayed.
7. If the host does not pass the endpoint compliance policy requirements, a remediation web page appears and directs the guest to correct the problems that inhibited opening his account.

Using a kiosk

A sponsor is an individual who is granted permission by an administrator to create accounts for guests or contractors. If you are a kiosk sponsor, you log in to a self-serve kiosk with your credentials and display the self-serve web page.

Depending on the parameters defined in the Kiosk administrator profile by the administrator, the kiosk may only be available on specified days of the week during certain times of the day. As long as you, the kiosk sponsor, remain logged onto the kiosk, guests can create their own accounts. It is strongly recommended that you use a kiosk browser. Kiosk browsers block users from accessing other programs on the host or other web sites.

The required data for guest accounts is pre-defined by the administrator in the Guest template. The required data may include a guest's name, e-mail, and address. Once guests have created their accounts they can go anywhere within the facility to access the network.

A self serve kiosk:

- Reduces a sponsor's workload because guests create their own accounts.
- Frees up IT staff from having to create accounts.

- Makes it easier for guests visiting short-term to have network access.
- Allows guests immediate network access without depending on someone to do it for them.

To set up your kiosk:

1. Install a Kiosk browser on the computer being used as the kiosk. See [Kiosk browser on page 186](#).
2. If you plan to have guests print out their credentials, make sure that printer settings are correct for printing guest badges with login information. See [Printer settings for guest badges on page 184](#).
3. If you plan to allow guests to send credentials to a mobile telephone using an SMS message the following requirements must be met:
 - The guest template associated with the kiosk administrator profile must have Send SMS enabled and Mobile Number and Mobile Provider must be included in the data fields required for the guest account.
 - Enable the Mobile Providers that guests might be using in the Mobile Provider view. See [Mobile providers on page 1](#).
4. Create a guest template that will be used in the Kiosk. The settings in this template control all aspects of the guest account created through the kiosk. See [Create templates on page 167](#).
5. Create an administrator profile that permits only kiosk access and associate the kiosk guest template. See [Add a guest kiosk profile on page 177](#).
6. Create a new administrator and apply the Kiosk administrator profile to that user.
7. When the Kiosk user has been created, have the that user log into the computer being used as the kiosk. See [Log into a kiosk on page 186](#).

You are now ready to allow guests to create their own accounts.

Kiosk browser

Many browsers can be set to Kiosk mode to prevent access to everything on the computer on which the browser is running. If your guests will be creating their own network accounts on a publicly available computer, it is recommended that you install a browser that can run as a Kiosk browser. The example and instructions show below are for Firefox. Many other browsers have similar capabilities.

1. Download and install Firefox.
2. Download and install the Real Kiosk add-on.



Once the Real Kiosk add-on is installed, this browser will always run in Kiosk mode.

3. To close Firefox once it is in Kiosk mode type **Alt+F4**.
4. To go to the homepage type **Alt+Home**.
5. To temporarily access Firefox in normal mode, right-click on the Firefox icon and select Properties. In the **Target** field go to the end of the path, add `safe-mode` and click **OK**.
6. Launch Firefox.

Log into a kiosk

As an administrator, your administrator has enabled Kiosk Mode in your administrator profile. This means that once you have logged into a self-serve kiosk, guests can create their own accounts. Guests have access to the network according to the parameters defined by your administrator in the Guest template.

The use of a kiosk browser is recommended to prevent the guests or contractors from logging out and to provide more security.

1. Bring up a web browser and type in the URL: `http://<Hostname>:8080`
2. This brings you to the administrator login screen.
3. Enter the Username and Password given to you by your Administrator. The Kiosk Welcome Message Screen appears. Guests also see this Welcome screen.
4. A screen appears with **Information Required to Create an Account**.
5. From this screen, guests can create their own accounts.

Account creation

1. A guest sees a welcome screen with instructions supplied by the administrator.
2. The guest clicks **Start** in the welcome screen.
3. A screen opens with a form. Guests must enter their e-mail address, but the other information may be entered upon their arrival or later, when they activate their account.

Parameter	Description
E-mail	The guest's e-mail address. This becomes the guest's user name for logging on to the network. It is also used to email credentials if desired. Required.
Account Start Date	In Kiosk mode, the date and time cannot be changed. The account end date is determined by the duration entered in the kiosk template specified in the kiosk administrator profile. Accounts will never remain active beyond 11:59 PM each day.
Account End Date	If no duration is specified in the template or if the duration extends beyond midnight, the account will expire at 11:59 PM on the current day. If the duration ends before midnight, the account will expire at the specified time.
Additional Account Information	Guests enter Additional Account Information to create an account. The asterisk (*) indicates required fields. Note that the fields that appear in this screen were predefined in the template.
Mobile Number Mobile Provider	If you intend to allow guests to send themselves an SMS message with their login credentials, these two fields must appear on the Kiosk window.

4. The guest clicks **Apply**, which opens an account details screen containing the guest's e-mail and a generated password. Depending on the configuration of the template used to create the account, guests can print out their credentials so they have password available when they log in later, they can email credentials to themselves or they can send an SMS message to their mobile telephones.
5. Click **Finish**.

Account activation

The following procedure describes the steps guests follow to activate their temporary account on their own regardless of how it was created. Guest accounts can be created either by an administrator, a sponsor, or the guest themselves using a kiosk. Once the guest has received his login credentials through one of these account creation methods, the activation process is as follows:

1. Guests type in their e-mail address and the password that was generated when the account was created.
2. Guests click **Register** or **Download**.

3. The Welcome screen opens.
4. The account information in this screen may be filled in if guests entered the data when they arrived. If they did not, they need to do so at this time to create their account. The fields denoted with an asterisk (*) are the pre-defined required fields.
5. Guests click **Continue**. After a few moments, a pop-up screen appears with the FortiNAC Dissolvable Agent .exe file. Guests save this file on their computer.
6. Once guests are at the location in the facility where they will use their computer, they must run the .exe file, which scans their computer. The guest receives a pass or fail message.
7. If the host does not pass the policy requirements, a remediation web page appears and directs the guest to correct the problems that inhibited opening his account.
8. If the computer passes, the .exe file is automatically removed. Now the guest can go anywhere in the facility and connect to the network.

Kiosk shut down

A self-serve kiosk is shut down when the specified login period for the kiosk sponsor has elapsed. Guests will no longer be able to create their own accounts until the kiosk sponsor logs back into the kiosk. During the period that the kiosk is shut down, guests should be directed to contact the help desk for account creation.

Guest self registration

Use the self registration feature to allow a guest to create a request for access to your network from their own device. When the guest opens a browser he is redirected to the registration page in the captive portal. From that page he can either login with previously assigned credentials or request access. Requests are forwarded to a sponsor or to a request pool to be approved or denied. When a request is approved, the guest receives his credentials in the browser on the login page, in an email or in an SMS message sent to his mobile telephone. All guest accounts are configured to expire after a user specified amount of time based on the template with which they are created.

End user workflow

Steps

1. Connect to the network.
2. Open a browser. The Isolation message is displayed briefly.
3. The browser is redirected to the Registration page.
4. On the Registration page, click the **Self Registration** option. A request form is displayed.
5. Fill in the form and click **Request Guest Access**. Depending on the configuration of the web page, you may be required to enter the email address of a sponsor. A sponsor is a person who has access to the FortiNAC administration program and can approve or deny your access request.
6. The browser displays a welcome message and asks you to wait. You can click **Cancel** if you wish to cancel the request.
7. The request expires if it is not responded to within the number of minutes configured in the portal. The default is 20 minutes.
8. When the sponsor approves the request, you are taken to the **Login** screen. Depending on the portal configuration, credentials are filled in automatically, they are sent to the guest via email and in an SMS message.
9. Click **Login** on the Welcome page. The Success page is displayed.

10. A message is displayed indicating that your network is being reconfigured and to close and reopen the browser. Close the browser and reopen it. You are now on the Production network and should be able to access the internet freely.
11. If you shut down your computer and access the network again later, you must open a browser and login again. If cookies are enabled on your computer, the login screen is displayed and the User Name and Password fields may be pre-populated.

Implementation

It is recommended that you review the Implementation process for guest manager for general setup details. This section covers only those configuration details that are specifically required for Guest self registration.

- All guest accounts are created based on a template. For guest self registration you must create a template with **Visitor Type** set to **Self-Registered Guest** and it must have an account duration to indicate when the account should expire. There is a default template, GuestSelfRegistration, that can be used or you can create a new one. All Self-Registered guests are configured with the same template. The template used is selected in the Portal content editor under **Registration > Self Registration Login**.
- Create an administrator profile specifically for administrators that will respond to Guest self registration requests these users could also have permission for guest/contractor accounts or other parts of FortiNAC that you deem appropriate for their job. See [Add a guest self registration profile on page 178](#).
- Create one or more administrator that will be responsible for processing Guest self registration requests and apply the Guest self registration profile. Administrators must have an e-mail address if they are to receive and respond to requests for guest accounts. Note that administrators can be created based on groups in your directory and permissions or profiles can be automatically assigned based on those groups. This can be useful if many people in your organization will be responsible for processing Guest self registration requests. See [Set privileges based on directory groups on page 149](#).
- Configure your portal pages for Guest self registration in the portal content editor. See [Portal page setup on page 182](#).
 - Within the Portal you can specify the sponsor or sponsors to which the request should go or you can enable the **Sponsor** field for the guest to fill in when creating the request. The guest must enter the sponsor's email address.
 - If you do not enable the **Require Sponsor Approval** option for guest accounts, guests simply create their own accounts using the template specified in the portal.
- If you require sponsors and other administrators to connect to the admin UI using https or if you are in a high availability environment where redundant servers do not share an IP address because those servers are on different subnets you must configure settings to generate the correct links in the emails sent to sponsors.

Sponsor Approval Email Links

In Guest Manager when Self Registration Requests are sent to sponsors, the email messages contain links for the sponsor to either automatically accept/deny the request, or to login to the Admin UI to do this. The default links provided use https access and authenticate against the SSL certificate securing the FortiNAC Admin UI.

Modifying Host Name, Security Level and Port

The link contained in the email is composed by FortiNAC. The link contains the URL of the FortiNAC Server. Any of the following URL components can be modified:

- FQDN (default: FQDN as appears in /etc/hosts file and Configuration Wizard Basic Network screen)
- Security Level (default: https)
- Port (default: 8443)

In some situations, it may be desired to modify any or all of these components depending upon the appliance configuration. For example, in a High Availability environment with an L3 configuration where redundant FortiNAC servers do not use a shared IP address, the URL should contain the FQDN of the correct FortiNAC Server. Typically, FortiNAC can determine the FQDN; however if there is an issue, the FQDN can be configured.

To modify any of the above components for the email links, a property file must be modified on the FortiNAC Server. Modify the property file as follows on both Primary and Secondary Servers:

1. Log into the CLI as root on your FortiNAC Server.
2. Navigate to the following directory: `/bsc/campusMgr/master_loader/`
3. Using vi or another editor, open the `.masterPropertyFile` file.
4. At the top of the file there is a sample entry that is commented out. Use the syntax and below to create your own changes.

Syntax:

```
FILE_NAME=./properties_plugin/selfRegRequest.properties
{
com.bsc.plugin.guest.SelfRegRequestServer.EmailLinkHost=<security
level>://<FQDN>:<port>
}
```

Example:

```
#####
# FILE_NAME=./properties_plugin/bridgeManager.properties
# {
# com.bsc.plugin.bridge.BridgeManager.verifyRegisteredClients=true
# }
#####
FILE_NAME=./properties_plugin/selfRegRequest.properties
{
com.bsc.plugin.guest.SelfRegRequestServer.EmailLinkHost=https://myNACServer.Fortinetnetworks.com:8443
}
```

5. Save the changes to the file.
6. Restart the FortiNAC Server.
shutdownCampusMgr
<wait 30 seconds>
startupCampusMgr
 When the server restarts, the changes listed in the `.masterPropertyFile` are written to the `selfRegRequest.properties` file.

Verify:

Log into the CLI of the FortiNAC Server and verify that the changes have been written to `selfRegRequest.properties`. At the prompt, enter:

```
grep -i EmailLinkHost /bsc/campusMgr/master_loader/properties_
plugin/selfRegRequest.properties
```

Now when FortiNAC sends sponsor approval email, the links included will use this modified URL.

Account requests

Use the account requests view to manage requests submitted when users attempt to register through any of the following portals requiring approval:

- Standard User Registration Approval
- Guest User Registration Approval
- Custom User Registration Approval

See [Registration](#) for configuration details.

The table shows requests based on the search parameters entered, including pending requests that have yet to be processed. Pending requests are approved or denied from this view.

To access the view select **Users & Hosts > Account requests**.

Settings

Field	Definition
Request Date	Date and time the request was received.
Response Date	Date and time that either the sponsor or the server responded to the request. For example, if the request expires, the server sends a message to the guest advising that the request expired.
Response Expiration	Date and time that the request expires. This is calculated based on the expiration settings in the Portal Contents Editor under Registration > Self Registration Login .
Sponsor	User name of the sponsor or the administrator who processed the request. For pending requests it is the user name of the sponsor to whom the request was sent.
IP address	IP address of the host associated with the guest who sent the request.
Physical Address	MAC address of the interface with which the host connected to the network.
Location	The name of the device and port where the guest is connected to the network.
User ID	User name of the guest requesting network access.
State	State of the request. Includes: Accepted, Canceled, Denied, Error, Expired or Pending.
Information	Contains text such as messages sent by the sponsor to the guest or the reason for an error state.
Buttons	
Show Details	Displays the Details Panel for the selected request. If the request is pending, allows you to approve or deny the request.

Details

The Details dialog displays information about a request for access sent by a guest user from the self registration page in the portal. If the request is still pending, the details window is used to approve or deny the request. If the request has been processed or has expired, the details window shows the history of the request.

View or process a request

1. From the menu bar select **Users & Hosts > Registration Requests**.
2. Use the Filters to locate the request you want to view or process.
3. Select the appropriate request from the list and click **Show Details**.
4. If this is a pending request, click **Approve** or **Deny** to process it.
5. If this is a request that has already been processed, view the details and then click **Hide Details** to close the window.

Approve or deny a request

When a guest connects to your network and selects self registration from the Registration page in the portal, a request for an account is sent to FortiNAC. The request is sent via email to a sponsor for approval; however an Administrator can go to the self registration requests View and approve or deny any pending requests.

1. A guest connects to the network, opens a browser and is taken to the Registration page. The guest submits a request for access.
2. The sponsor receives an email indicating that a guest has requested an account. Within the email there is either a Login link or Approve and Deny links depending on the configuration of the self registration page in the portal.
3. If the email contains Approve or Deny links, the sponsor clicks the appropriate link. The Guest receives a message indicating that he has been approved or denied. If the request is approved, the guest can login and use the network.
4. If the email contains a Login link, the sponsor clicks **Login** and is taken to a login window for the FortiNAC admin UI.
5. The sponsor logs in and the self registration requests view is displayed with the appropriate request record opened.
6. The sponsor can add a message indicating what the Guest should do or the reason for a denied request. This message is displayed to the guest in the browser.
7. The sponsor clicks **Approve** or **Deny** and the response is sent to the Guest.
8. If approved, the Guest can access the network.

Registration requests

Use the Registration Requests view to manage requests submitted when users attempt to register through the Self Registration portal when requiring approval. See [Registration](#) for configuration details.

To access the view, select **Users & Hosts > Registration Requests**.

Settings

Field	Definition
State	State of the request. Includes: Accepted, Canceled, Denied, Error, Expired or Pending.
IP Address	IP address of the host associated with the guest who sent the request.
MAC Address	MAC address of the interface with which the host connected to the network.
Location	The name of the device and port where the guest is connected to the network.

Field	Definition
Device Owner	User name of the guest requesting network access.
Request Date	Date and time the request was received.
Expiration Date	Date and time that the request expires. This is calculated based on the expiration settings in the Portal Contents Editor under Registration > Self Registration Login .
Request Approver	User name of the sponsor or the administrator who processed the request. For pending requests it is the user name of the sponsor to whom the request was sent.
Response Date	Date and time the request was received.
Request Key	A unique identifier for the request, so it may be differentiated from other requests.
Request Source	Which section of the product was used to generate the Registration Request. Current possible values are: • Portal - Standard User Login • Portal - Guest Login • Portal - Custom Login
Request Source Name	Contains the name of the Portal that was used to generate the registration request.
Buttons	
Approve	Approve a request
Deny	Deny request
Delete	Delete request

View or process a request

1. From the menu bar select **Users & Hosts > Registration Requests**.
2. Use the Filters to locate the request to view or process.
3. Select the appropriate request from the list and click Show Details.
4. If this is a pending request, click **Approve** or **Deny** to process it.

User accounts

Use this view to add, delete, modify, locate and manage users on your network. Users include network users, guest or contractor users and Administrators. Administrators can also be managed from the administrators view. Administrator are also network users, therefore, they are included in the users view with a slightly different icon. See [Icons on page 44](#) for information on each icon.

If you have an LDAP or Active Directory configured, user information is added from the directory as users register on the network. The FortiNAC database is periodically synchronized with the directory to make sure that data is the same in both places. User information from the directory is matched to user information in the FortiNAC database based on user ID. If you manually create a user with an ID that is the same as a user in the directory, then directory data will overwrite your manually entered data.

The relationship between users, hosts, and adapters is hierarchical. Users own or are associated with one or more hosts. Hosts contain one or more Adapters or network interfaces that connect to the network. For example, if you search for a host with IP address 192.168.5.105, you are in fact searching for the IP address of the adapter on that host. When the search displays the host, you can click on the Adapters tab, the search is automatically re-run and you see the adapter itself. If there is an associated user, you can click on the Users tab to re-run the search and see the associated user.

Click on the arrow in the left column to drill-down and display the hosts associated with the selected user. Hover over the icon in the Status column to display a tooltip with detailed information about this user. For settings, see [Search settings on page 199](#).

Settings

Field	Definition
Address	User's street address.
Allowed Hosts	The number of hosts that can be associated with or registered to this user and connect to the network. There are two ways to reach this total. If the host is scanned by an agent or if adapters have been manually associated with hosts, then a single host with up to five adapters counts as one host. If the host is not scanned by an agent or if the adapters have not been associated with specific hosts, then each adapter is counted individually as a host. In this scenario one host with two network adapters would be counted as two hosts. Numbers entered in this field override the default setting in System > Settings > Network Device. Blank indicates that the default is used. See Network device on page 910. If an administrator exceeds the number of hosts when registering a host to a user, a warning message is displayed indicating that the number of Allowed Hosts has been incremented and the additional hosts are registered to the user.
City	User's city of residence.
Created Date	Date the user record was created in the database. Options include Before, After, and Between.

Field	Definition
Delete Hosts When User Expires	Indicates whether hosts registered to this user should be deleted from the database when the user's record ages out of the database.
Email	User's email address.
Expiration Date	Controls the number of days a user is authorized on the network. Options include Before, After, Between, Never, and None. The user is deleted from the database when the date specified here has passed. The date is automatically calculated based on the information entered when Aging is configured. See Aging out host or user records on page 241 .
Delete Hosts When User Expires	Indicates whether hosts owned by this user should be deleted when the user ages out of the database. It is recommended that you set this to Yes.
Inactivity Date	Controls the number of days a User is authorized on the network. Options include Before, After, Between, Never, and None. User is deleted from the database when the date specified here has passed. The date is continuously recalculated based on the information entered in the Days Inactive field. See Aging out host or user records on page 241 or Set user expiration date on page 208 .
Inactivity Limit	Number of days the user must remain continuously inactive on the network to be removed from the database. See Aging out host or user records on page 241 or Set user expiration date on page 208 .
Last Login/Logout	Date of the last time the user logged into or out of the network or the FortiNAC admin UI. This date is used to count the number of days of inactivity. Options include Before, After, Between, and Never.
Last Name	User's last name.
Mobile Number	User's mobile phone number. Can be used to send SMS messages based on alarms. Requires the Mobile Provider to send SMS messages.
Mobile Provider	Provider or carrier for user's mobile phone.
Notes	Notes about this user.
Phone	User's telephone number.
User Role	Role assigned to the user. Roles are attributes of users and are used as filters for user/host profiles. See Roles on page 620 .
User Security & Access Value	Value that typically comes from a field in the directory, but can be added manually. This value groups users and can be used to determine which role to apply to a user or which policy to use when scanning a user's computer. The data in this field could be a department name, a type of user, a graduation class, a location or anything that distinguishes a group of users.
State	User's state of residence.
Status	Current or last known status is indicated by an icon. See Icons on page 44 . Hover over the icon to display additional details about this User in a tool tip. Access: Indicates whether user is enabled or disabled.

Field	Definition
Title	User's title, this could be a form of address or their title within the organization.
Type	Type of user. Allows you to differentiate between network users and guest/contractor users.
User ID	Unique alphanumeric ID. If you are using a directory for authentication, this should match an entry in the directory. If it does not, FortiNAC assumes that this user is authenticating locally and asks you for a password. When using a directory for authentication, fields such as name, address, email, are updated from the directory based on the user ID when the database synchronizes with the directory. This is true regardless of how the user is created and whether the user is locally authenticated or authenticated through the directory. If the user ID matches a user ID in the directory, the FortiNAC database is updated with the directory data.
Postal Code	User's zip code based on their state of residence.
Last Modified By	User name of the last user to modify the user.
Last Modified Date	Date and time of the last modification to this user.

Navigation, menus, options, and buttons

For information on selecting columns displayed in the user view see [Configure table columns and tooltips on page 197](#). Some menu options are not available for all Users. Options may vary depending on user state.

Field	Definition
Quick Search	Enter a single piece of data to quickly display a list of users. Search options include: IP address, MAC address, host name, User Name, and user ID. Drop-down arrow on the right is used to create and use custom filters. If you are doing a wild card search for a MAC address you must include colons as separators, such as 00:B6:5*. Without the separators the search option cannot distinguish that it is a MAC address. When quick search is enabled, the word Search appears before the search field. When a custom filter is enabled, Edit appears before the search field.
Right click options	
User Properties	Opens the Properties window for the selected user. See User properties on page 200 .
Add Users To Groups	Add the selected user(s) to one or more group(s). See Add users to groups on page 205 .
Delete Users	Deletes the selected user(s) from the database. See Delete a user on page 204 .
Disable Users	Disables the selected user (s) preventing them from accessing the network regardless of the host they are using. Hosts registered to a disabled user will remain disabled regardless of the logged on user (if different).
Enable Users	Enables the selected user(s) if they were previously disabled. Restores network access.
Group Membership	Displays groups in which the selected user is a member.

Field	Definition
	If the User is also an administrator, separate options are displayed for administrator Groups and User Groups. Options are Group Membership (User) and Group Membership (Administrator) .
Guest Account Details	Displays account details for the selected guest record, such as: user ID, account status, sponsor, account type, start and end dates, availability, role, authentication, security policy, account duration, reauthentication period, success URL, and the guest's password. See Guest account details on page 207 .
Modify User	Opens the Modify User window. See Add or modify a user on page 202 .
Policy Details	Opens the Policy Details window and displays the policies that would apply to the selected user at this time, such as endpoint compliance policies, network access policies or Supplicant Policies. See Policy details on page 461 .
Set Expiration	Launches a tool to set the date and time for the user to age out of the database. See Set user expiration date on page 208 .
Set Role	Assigns a role to the selected user. See Roles on page 620 .
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746 .
	 You must have permission to view the admin auditing log. See Add an administrator profile on page 139.
Show Events	Displays all events for the selected user.
Collapse All	Collapses all records that have been expanded.
Expand Selected	Expands selected user records to display host information.
Buttons	
Import/Export	Import and Export options allow you to import users into the database from a CSV file or export a list of selected hosts to CSV, Excel, PDF, or RTF formats. See Import hosts, users or devices on page 102 or Export data on page 116 .
Options	Displays the same series of menu picks displayed when the right-mouse button is clicked on a selected user.

Configure table columns and tooltips

Use the configuration button  on the **User View**, **Adapter View**, **Host View**, and **Applications View** to open the **Settings** window. The settings window controls the columns displayed in each view and the details displayed in tooltips when you hover over an icon.

Table columns

1. Click **Configuration**.
2. When the Settings window displays, select the **Table Columns** tab.
3. Mark the columns to be displayed in the table on the User, Adapter or **Host View** with a check mark and click **OK**.
4. These settings are saved for the logged in user.

Tooltips

Select the fields to be displayed in the tooltip when you hover the mouse over the status icon of either a User, an Adapter, or a Host. Available fields vary depending on which item you are configuring.

1. Click **Configuration**.
2. When the Settings window displays, select the **Table Tooltip** tab.
3. The **Available Fields** column displays fields that can be displayed, but have not yet been selected. The **Selected Fields** column displays fields that will display in the tooltip.
4. Use the arrows in the center of the window to move fields from one column to the other until the appropriate set of fields is displayed in the **Selected Fields** column.
5. Select a field in the **Selected Fields** column and use the up and down arrows to change the order of display. Use the **Sort** button to sort fields alphabetically.
6. The **Hide Blank Fields** option is enabled by default. It reduces the size of the tooltip when selected fields are blank for a particular item. For example, if you have selected **Host Expires** and the selected Host does not have an expiration date, then when the tooltip for that host is displayed, the **Host Expires** field is hidden.
7. Click **OK** to save your changes. These settings are saved for the logged in user.

Using tooltips

Tooltips are displayed when you hover the mouse over a status icon in the **User**, **Adapter**, or **Host Views**. Tooltip details are configured using the Settings window shown in the previous section.

 00:11:43:52:7C:AD	 
IP Address:	192.168.10.173
Physical Address:	00:11:43:52:7C:AD
Location:	Concord-3750 Fa2/0/44
Host Name:	outrigger

- When a tooltip is displayed, click the Push Pin icon to anchor it to the screen. Now you can move the tooltip around your desktop without it closing.
- High-light text in a tooltip and press Ctrl-C to copy it. Press Ctrl-V to paste the text in a field.
- Open and anchor multiple tooltips to quickly compare data.
- Hover over the status icon in the top left corner for text based status information.

Search settings

The fields listed in the table below are displayed in columns on the user view based on the selections you make in the Settings window, see [Configure table columns and tooltips on page 197](#). Most of these fields are also used in custom filters to search for hosts. Additional fields that can be displayed on the user view are fields for the host associated with the selected user, see [Settings on page 216](#).

You may not have access to all of the fields listed in this table. Access depends on the type of license key installed and which features are enabled in that license.

Field	Definition
Access	Indicates whether host is enabled or disabled
Address	Users's street address.
City	User's city of residence.
Created Date	Date the user record was created in the database. Options include Last, Between, Before, and After.
Email	User's email address.
Expiration Date	Controls the number of days a user is authorized on the network. Options include: next, before, after, between, never, and none. The user is deleted from the database when the date specified here has passed. The date is automatically calculated based on the information entered when aging is configured. See Aging out host or user records on page 241 .
First Name	User's first name.
Inactivity Date	Controls the number of days a user is authorized on the network. Options include next, before, after, between, never, and none. User is deleted from the database when the date specified here has passed. The date is continuously recalculated based on the information entered in the Days Inactive field. See Aging out host or user records on page 241 or Set user expiration date on page 208 .
Inactivity Limit	Number of days the user must remain continuously inactive on the network to be removed from the database.
Last Login/Logout	Date of the last time the user logged into or out of the network or the FortiNAC admin UI. This date is used to count the number of days of inactivity. Options include Last, Before, After, Between, and Never.
Last Name	User's last name.
Mobile Number	User's mobile phone number. Can be used to send SMS messages based on alarms. Requires the mobile provider to send SMS messages.
Mobile Provider	Provider or carrier for user's mobile phone.
Notes	Notes about this user.
Phone	User's telephone number.

Field	Definition
Role	Role assigned to the user. Roles are attributes of users and are used as filters for user/host profiles. See Roles on page 620 .
Security & Access Value	Value that typically comes from a field in the directory, but can be added manually. This value groups users and can be used to determine which role to apply to a user or which policy to use when scanning a user's computer. The data in this field could be a department name, a type of user, a graduation class, a location or anything that distinguishes a group of users.
State	User's state of residence.
Title	User's title, this could be a form of address or their title within the organization.
Type	Type of user. Allows you to differentiate between network users and guest/contractor users.
User ID	Unique alphanumeric ID. If you are using a directory for authentication, this should match an entry in the directory. If it does not, FortiNAC assumes that this user is authenticating locally and asks you for a password. When using a directory for authentication, fields such as name, address, email, are updated from the directory based on the user ID when the database synchronizes with the directory. This is true regardless of how the user is created and whether the user is locally authenticated or authenticated through the directory. If the user ID matches a user ID in the directory, the FortiNAC database is updated with the directory data.
Postal Code	User's zip code based on their state of residence.

User properties

The User Properties view provides access to detailed information about a single user. From this view you can access the associated host by clicking on the adapter's physical address displayed in the Registered Hosts tab at the bottom of the window.

Access user properties

1. Select **Users & Hosts > User Accounts**.
2. Search for the appropriate user.
3. Select the user and either right-click or click **Options**.
4. From the menu, select **User Properties**.

Settings

Field	Description
General	
First Name	User's first name.
Last Name	User's last name.

Field	Description
ID	Unique alphanumeric ID for this user. Typically comes from the directory but if you are not using a directory, this field can be created manually. This field cannot be modified. When using a directory for authentication, fields such as name, address, and email, are updated from the directory based on the user ID when the database synchronizes with the directory. This is true regardless of how the user is created and whether the user is locally authenticated or authenticated through the directory. If the user ID matches a user ID in the directory, the FortiNAC database is updated with the directory data.
Title	User's title, this could be a form of address or their title within the organization.
Role	Role assigned to the user. Roles are attributes of users that can be used as filters in user/host profiles. See Roles on page 620 .
Security And Access Attribute Value	Value that typically comes from a field in the directory, but can be added manually. This value can be used as a filter to determine which policy to use when scanning a user's computer. The data in this field could be a department name, a type of user, a graduation class, a location or anything that distinguishes a group of users.
User Status	Radio buttons indicating whether the user is Enabled or Disabled. To enable or disable the user, click the appropriate button and then click Apply.
Allowed Hosts	The number of hosts that can be associated with or registered to this user and connect to the network. There are two ways to reach this total. If the host is scanned by an agent or if adapters have been manually associated with hosts, then a single host with up to five adapters counts as one host. If the host is not scanned by an agent or if the adapters have not been associated with specific hosts, then each adapter is counted individually as a host. In this scenario one host with two network adapters would be counted as two hosts. Numbers entered in this field override the default setting in System > Settings > Network Device. Blank indicates that the default is used. See Network device on page 910. If an administrator exceeds the number of hosts when registering a host to a user, a warning message is displayed indicating that the number of Allowed Hosts has been incremented and the additional hosts are registered to the user.
Time	
Expiration Date	Controls the number of days a user is authorized on the network. User is deleted from the database when the date specified here has passed. The date is automatically calculated based on the information entered in the Set User Expiration date window. To modify click Set . See Set user expiration date on page 208 for additional information.
Inactivity Date	Controls the number of days a user is authorized on the network. User is deleted from the database when the date specified here has passed. The date is continuously recalculated based on the number of days entered for Inactivity Limit.

Field	Description
	For example, if the user logs off the network on August 1st and Inactivity Limit is set to 2 days, the Inactivity Date becomes August 3rd. If on August 2nd the user logs back in again, the Inactivity Date is blank until the next time he logs out. Then the value is recalculated again. To modify click Set .
Inactivity Limit	Number of days the user must remain continuously inactive to be removed from the database. See Aging out host or user records on page 241 .
Last Login/Logout	Date of the last time the user logged into or out of the network or the FortiNAC admin UI. This date is used to count the number of days of inactivity.
Delete Hosts Upon Expiration	If set to Yes, hosts registered to the user are deleted when the user ages out of the database. To modify click Set .
Created	Indicates when this record was created in the database.
Tabs	
Registered Hosts	Displays a list of hosts, by the MAC address of their adapters, registered to this user. Click on a MAC address to open the Host Properties.
Logged In Hosts	List of hosts by host name registered to this user that are currently logged onto the network.
Notes	Notes entered by the administrator. If this user registered as a guest, this section also contains information gathered at registration that does not have designated database fields, such as Person Visiting or Reason for Visit.
Buttons	
Apply	Saves changes to the user properties.
Reset	Resets the values in the User Properties window to their previous settings. This option is only available if you have not clicked Apply .

Add or modify a user

User records are created as users connect to the network and register. Users can be added by importing them in a file or by entering the data manually. See [Import and export data on page 101](#). The Add or Modify User feature allows you to create new users or edit existing ones.

1. Select **Users & Hosts > User Accounts**.
2. Click **Add**.
3. In the **Enter User ID** window type a unique alphanumeric ID for this user. If you are using a directory for authentication, enter the user ID from the directory. This allows FortiNAC to synchronize its database with the directory and update user data.
4. Click **OK**. FortiNAC verifies that the user ID is in the directory and populates fields that have existing data in the directory, such as First and Last Name.
5. If the user is not in the directory, you can still add the user, but FortiNAC assumes that this user will authenticate locally and asks you for a password for the user.
6. **To modify an existing user**, use the search or filter mechanisms on the **User View** to locate the appropriate user.

7. Click on the user to select it.
8. Click **Modify**.
9. See the table below for detailed information on each field.
10. Click **OK** to save your data.

Settings

Field	Definitions
Required fields	
User ID	
Change Password	Allows you to change the password for this user. Users who authenticate through the directory will not have a Change Password button. Only users who are locally authenticated by FortiNAC have a change password option.
First Name Last Name	User's name as it is retrieved from the directory. If you are using a directory, these fields are updated every time the directory is re-synchronized with the database. If you are not using a directory, enter the user's first and last name.
Role	Roles are attributes of users and can be used as filters in user/host profiles. These profiles are used to determine which network access policy, endpoint compliance policy or Supplicant EasyConnect Policy is applied.
Additional info	
Address	User's address of residence.
City	User's city of residence.
State	Two letter abbreviation for state of residence.
Zip/Postal Code	Postal code for the user's city and state of residence.
Email	User's email address. For multiple e-mail addresses, enter addresses separated by commas or semi-colons. Messages are sent to all e-mail addresses provided.
Title	This can be a form of address, such as Mr., or a title within the organization.
Mobile Number	Mobile Phone number used for sending SMS messages to guests and administrators.
Mobile Provider	Mobile provider for the mobile phone number entered in the previous field. Used to send SMS messages to guests and administrators. This field also displays the format of the SMS address that will be used to send the message. For example, if the provider is US Cellular, the format is xxxxxxxxx@emai.uscc.net, where the x's represent the user's mobile phone number. The number is followed by the email domain of the provider's message server.
Allowed Hosts	The number of hosts that can be associated with or registered to this user and connect to the network. There are two ways to reach this total. If the host is scanned by an agent or if adapters have been manually associated with hosts, then a single host with up to five adapters counts as one host. If the host is not scanned by an agent or if the adapters have not been associated with specific hosts, then each adapter is counted individually as a host. In this scenario one host with two network adapters would be counted as two hosts.

Field	Definitions
	Numbers entered in this field override the default setting in System > Settings > Network Device. Blank indicates that the default is used. See Network device on page 910. If an administrator exceeds the number of hosts when registering a host to a user, a warning message is displayed indicating that the number of Allowed Hosts has been incremented and the additional hosts are registered to the user.
Global Default	Default number of Allowed Hosts used if the Allowed Hosts field is empty. The default is set in System > Settings > User/Host Management > Allowed Hosts .
Notes	Free form notes entered by the Administrator.
Security and Access Attribute Value	This value is an attribute of users and can be used as a filter in user/host profiles. These profiles are used to determine which network access policy, endpoint compliance policy or Supplicant EasyConnect Policy is applied. If a directory is in use, the Security and Access Attribute value comes from the directory when it is synchronized with the database. Otherwise the value can be entered manually.
RADIUS - Local Password Validation (MSCHAPv2)	RADIUS MSCHAPv2 credential validation against local users Allows mschap module in FreeRADIUS service to authenticate user credentials without a query to a backend active directory. This option is only presented when the following global options is enabled in cli: run: <pre>execute enter-shell globaloptiontool -name "localRadiusServer.mschapV2LocalUserAuth" -set true</pre>

Delete a user

When you delete a user, you have the option to delete hosts registered to this user or leave them in the database. It is recommended that you delete the registered hosts. If they are not deleted, registered hosts associated with a deleted user become registered devices. If a user connects to the network with one of these devices, there is nothing to prevent network access because the device is known in the database.

1. Select **Users & Hosts > User Accounts**.
2. Use the **Quick Search** or **Custom Filter** to locate the appropriate user.
3. Select the user and click **Delete**.
4. A warning message is displayed asking if you would like to delete registered hosts associated with this user.
5. **To delete hosts**, enable the check box labeled **Delete Hosts Registered to User** and click **Yes**.
6. **To convert hosts to registered devices**, disable the check box labeled **Delete Hosts Registered to User** and click **Yes**.

Add users to groups

You can add selected users to groups you have created. See [Groups on page 843](#) for detailed information on Groups and how they are used in FortiNAC.

1. Select **Users & Hosts > User Accounts**.
2. Use the **Quick Search** or **Custom Filter** to locate the appropriate user(s).
3. Use Ctrl-click or Shift-click to select the records you wish to add to the group.
4. Right-click or click **Options** and select **Add Users To Groups**. The **Add Users to Groups** view lists the available user groups and sub-groups. Sub-groups are displayed under their parent group or groups.
5. To add the users to a group, click the box next to the group name and then click **OK**.
6. To create a missing group:
 - a. Click **Create Group**.
 - b. Enter a group name.
 - c. If the new group should be a sub-group of an existing group, enable the **Parent Group** option and select the appropriate group from the list.
 - d. **Description** is optional.
 - e. Click **OK** to save the new group.
7. Click **OK**.

Group membership

From the user view window you can view or modify the group membership of an individual user. Use this option to open a window that displays a list of all groups to which the selected user belongs.

1. Select **Users & Hosts > User Accounts**.
2. Use the **Quick Search** or **Custom Filter** to locate the appropriate user(s).
3. Click on a user to select it.
4. Right-click or click **Options** and select **Group Membership**.
5. The **Group Membership** view lists the available user groups and sub-groups. Sub-groups are displayed under their parent group or groups. A check next to a group name indicates that this user is contained in that group.
6. To add the user to a group, click the box next to the group name and then click **OK**.
7. To remove the user from a group, click to uncheck the box next to the group name and then click **OK**.
8. To create a missing group:
 - a. Click **Create Group**.
 - b. Enter a group name.
 - c. If the new group should be a sub-group of an existing group, enable the **Parent Group** option and select the appropriate group from the list.
 - d. **Description** is optional.
 - e. Click **OK** to save the new group.
9. Click **OK**.

Guest accounts

This option allows you to create accounts for guests visiting your facility. It provides a user name and password for each guest. Guests are authenticated through FortiNAC. Administrators, operators, and help desk users all have permission to create guest accounts.

The guest account option is not available if you are using the guest manager feature. The guest manager feature provides extensive guest creation and management options.

Add a guest account

Guest accounts can be viewed and modified in User Accounts. Guest accounts are provided with a default Security and Access value of "guest" allowing you to use this as a filter for user/host profiles. When a guest matches a profile the guest receives the endpoint compliance policy associated with that profile. You can use the same user/host profile to assign a network access policy and assign guest hosts to a VLAN. See [Policies on page 531](#) and [Network access on page 482](#) for additional information.

1. Select **User & Hosts > User Accounts**. Select **Create New**.
2. Enter an **ID**. This field is required.
3. Enter a **Password**. This field is required.
4. Select the guest role for the account in **Role**.
5. Enter the guest's **First** and **Last** names.
6. Click **OK** to save the guest account.

When a guest connects to the network and reaches the login page, the last name is used as the user name. If you are using the Version 1 Portal pages, you can edit the .html files directly to modify the labels on the fields on the login page. If you have disabled the Version 1 Portal pages and are using the portal pages that shipped with FortiNAC, the field labels can be modified using the content editor in the portal configuration window.

Portal page requirements

If you are using your Version 1 Portal pages and you already have guest pages set up, you do not need to make any modifications. If you have disabled the Version 1 Portal pages and chose to use the Portal pages provided with FortiNAC, there are a few fields that must be edited to allow guests to login using accounts created with the **Guest Account** tab on the dashboard. These options do not apply to guest accounts created with guest manager.



If you are using local authentication for guests, do not enable the First Name and Last Name fields on the Custom Login Form. Information entered by guests at login in these fields is added to the database and will modify their authentication credentials. Guests would no longer be able to log in with their original credentials.

Configure guest login

The Guest Login designated in the portal configuration content editor is used to configure settings for guest manager. If you are not using guest manager you must disable that login and enable the custom registration login.

1. Select **Portal > Portal Configuration**.
2. Click on **Registration**.
3. Click on **Login Menu**. The properties for that page are displayed in the right pane.
4. Scroll down to the **Guest Login Enabled** check box and remove the check mark.
5. Scroll to the **Custom Registration Enabled** check box and mark it with a check mark.
6. Scroll to the **Custom Registration Link Text** field and enter the text for the link to the guest login page, such as guest login or guest registration.
7. Scroll to the **Custom Registration Title** field and enter the text that should display above the link to the guest login page.
8. Click **Apply** to save your changes. When changes are made to the portal pages there is a delay before the changes are displayed.

Configure guest authentication

1. Select **Portal > Portal Configuration**. See [Portals](#).
2. Click on **Global** in the left hand pane to expand it.
3. Click on **Settings** within Global. The properties for that page are displayed in the right pane.
4. Scroll down to **Custom Login Type** and select **Local** from the drop-down menu.
5. Click **Apply** to save your changes. When changes are made to the portal pages there is a delay before the changes are displayed.

Modify user name field label

When guest accounts are created, the guest's last name is considered the User Name for login. The Login page asks for User Name and Password. You can either advise your guests that their last name is their user name or you can modify the Login page and set the label appropriately.

1. Select **Portal > Portal Configuration**
2. Click on **Registration**.
3. Click on **Custom Login Form**. The properties for that page are displayed in the right pane.
4. Scroll to the **User Name Field Label** field and change the label to Last Name or some other user-specified name.
5. Click **Apply** to save your changes. When changes are made to the portal pages there is a delay before the changes are displayed.

Guest account details

Guest user records created when guest accounts are generated are displayed in the user view with network and administrator users. The **Guest Account Details** window displays data from the guest template used to create the guest user.

1. Select **Users & Hosts > User Accounts**.
2. Search for the appropriate user.
3. Select the user and either right-click or click **Options**.
4. From the menu select **Guest Account Details**.

Settings

Field	Description
User ID	Guest's email account which is used as the user ID at login.
Account Status	Indicates whether the guest account is enabled or disabled.
Sponsor	The administrator who created the guest account.
Account Type	Guest account type. Types include: • Guest: A visitor to your facility with limited or Internet-only network access. • Conference: A group of short- or long-term visitors to your organization who require identical but limited access to your network for typically one to five days. • Contractor: A temporary employee of your organization who may be granted all or limited network access for a specific time period generally defined in weeks or months.
Start Date	Date and time (using a 24-hour clock format) the account will become active for the guest or contractor.
End Date	Date and time the account will expire.
Login Availability	Times during which the guest is permitted to access the network.
Role	Role is an attribute of a user or a host. It is used in User/Host Profiles as a filter when assigning network access policies, endpoint compliance policies, and Supplicant EasyConnect policies.
Authentication	Indicates type of authentication used. Options include: Local, LDAP or RADIUS. Guests typically use Local authentication.
Account Duration	Amount of time this account will remain valid and usable.
Reauthentication Period	Number of hours the guest or contractor can access the network before reauthentication is required.
URL for Successful Landing Page	Directs the guest or contractor to a specific web page when they have successfully logged into the network and passed the scan in an endpoint compliance policy. This field is optional and is used only if you have Portal V1 enabled in portal configuration.
URL for Acceptable Use Policy	Directs the guest or contractor to a specific web page that details the acceptable use policy for the network.
Password	The Guest's assigned password. Passwords are usually generated by the system unless the guests were bulk imported. Toggle Show Password/Hide Password to alternately display the password in plain text or as asterisks.

Set user expiration date

The expiration date on a user determines when the user record is automatically deleted or aged out of the database. Administrators default to No Expiration. See [Aging out host or user records on page 241](#) for information on other methods.

The user inactivity timer is started when all hosts registered to a user are seen as offline. When a host is seen as connected, the timer is cleared. The timer is also cleared when the user logs into FortiNAC.

Administrators assigned the **System Administrator** profile cannot be aged out.

The Set User Expiration Date feature can be accessed either from the user view or the Host View.

1. Select **Users & Hosts > User Accounts**.
2. Use the **Quick Search** or **Custom Filter** to locate the appropriate user(s).
3. Select the users to be modified.
4. Right-click and select **Set Expiration**.
5. Use the table below to enter expiration criteria.
6. Click **OK** to set the expiration dates.

Settings

Field	Definition
Set Host Expiration	Enables the expiration date option and corresponding calculation methods.
Specify Date	Allows you to select a specific date that the host will be aged out of the database. Host age times are evaluated every ten minutes. If you specify a date and time, the host may not be removed from the database for up to ten minutes after the time selected.
Days Valid From Now	Enter the number of days (integer format) from today that you would like the host to expire. The expiration date is calculated based on this number.
Days Valid From Creation	This is the number of days (integer format) from the date the host record was created. The expiration date is calculated based on this number.
No Expiration	This host is never deleted from the database even if global or group aging options are added or modified.
Default Expiration	Defaults to the global aging settings configured in System > Settings > User/ Host Management > Aging .
Set Host Inactivity Limit	Enables the option to delete a host based on the number of days that it did not log onto the network.
Days Inactive	Number of consecutive days (integer format) the host must be inactive to be aged out of the database. For example, if this is set to 4 days, and after 2 days the host connects to the network again, the counter is restarted.
No Inactivity Limit	With this option enabled, the host is never deleted from the database due to inactivity even if global or group aging options are added or modified.
Default Inactivity Limit	Defaults to the global aging settings configured in System > Settings > User/ Host Management > Aging .

Maximum concurrent sessions



To correctly use this feature, users should turn on accounting port to get the correct number of sessions.



Supported authentication types

- Captive Portal without host logout
- VPN
- 802.1x/MAB
- Agent without logout/delete host

A limit can be set at Global level, in addition to User Level. There are two types of workflows:

1. Set limits globally

User can set maximum session limit globally from **Settings > User/Host Management > Allowed Hosts** page. Globally, both the following options will be available:

- Registered Host
- Logged in Host

This maximum concurrent session limit will be applied to all the users.

2. Set limits on User

The user can set maximum session limit on a particular user from **Users & Hosts > User Accounts** page. At User Level, both the following options will be available:

- Registered Host
- Logged in Host

This maximum concurrent session limit will be applied to the selected user.

Note: In case of Global and user settings conflict, the user settings will override the global settings for that particular user. This feature is not available for User Group, to avoid further conflict with the user settings.

Vulnerabilities

After a vulnerability service scanner is created and polling performed, vulnerability details will be shown on FortiNAC.

The integration of FortiNAC and Vulnerability Scanner is at **Network > Service Connector > Add New > Vulnerability Scanners**

(**Note:** For FortiNAC vF 7.6.3 and earlier version, the vulnerability previously listed in **System > Settings**. From the folder view of the display, click the **System Communications** node, and then click **Vulnerability Scanners**.)

For details, please refer to [Vulnerability Scanner Guide](#)

Hosts, adapters, and applications

Hosts are devices that require network services and can be associated with a user, such as a PC or a gaming device. Adapters are the network interfaces on these devices. There are other types of hosts not associated with users, such as IP phones or printers. The hosts, adapters, and users views provide an individual menu option for each, but uses a shared search capability to simplify management of hosts, adapters and their associated users on your network. Regardless of the menu item selected and displayed, the navigation and search or filter options are the same.

Applications that are contained on a host are scanned when the host is connected to the network, and appear in the applications view. The list of applications is continuously updated as hosts are scanned.

The quick search field at the top of the Host View and **Adapter View** windows allows you to search based on an IP address, MAC address, user ID, User First and Last Name or host name. Wild card searches, such as 192.168.10.1* can be used. The drop-down arrow at the end of the Search field allows you to set up a filter and use it once or save it for future use. See [Quick search on page 36](#) for additional information.

The mouse-over feature displays a pop-up window or tool tip when you place the mouse over any icon in the Status column. This tool tip contains detailed data about the user, host or adapter.

Add or remove columns from the table by clicking **Configuration** and selecting your options from **Settings**. **Settings** also controls the data included in tool tips displayed when you hover over any icon on the left side of the view.

USB/Thunderbolt external Ethernet adapters

The following information explains how FortiNAC manages records of hosts using external Ethernet adapters.

Thunderbolt adapters and docking stations

Thunderbolt Ethernet adapters are similar to USB Ethernet dongle adapters, but use the Thunderbolt connector.

Thunderbolt 2 docking stations have two Thunderbolt ports and one Ethernet port. This allows two computers to connect to the docking station using a Thunderbolt connection, but only one computer is able to have network access. The first computer to connect to the docking station is considered the "root user" and is associated to the Ethernet port. If a second computer connects to the docking station, it will not be able to access the network unless the first computer disconnects from the docking station.

FortiNAC treats the records of hosts connecting to this type of docking station (as well as the adapters) in the same manner as hosts using USB Ethernet dongle adapters.

Host record management when external adapters are moved between hosts

The Persistent Agent provides information regarding adapters enabled on the host. This allows FortiNAC to associate multiple adapters to the host record (not just the one connected during host registration). In conjunction with the Persistent Agent, FortiNAC is able to identify when an external adapter is moved from one host to another and update host records accordingly.

Hosts must have Persistent Agent installed and be communicating with Fortinet before moving the adapter. This will prevent the second host from inheriting the network access of the original host. In this case, the second host would appear as the original host and would not be detected.

For Persistent Agent configuration details, see [FortiNAC Persistent Agent Deployment and Configuration](#) in the Document Library.

If a host record contains only one adapter and the adapter is removed from the host, the host record is removed.

Adapters cannot be successfully moved between hosts using the Dissolvable Agent.

Adapter is moved between registered hosts

Example 1: Registered Host A (with Persistent Agent) to Registered Host B (with Persistent Agent):

Once the adapter is removed from Registered Host A and connected to Registered Host B, the Persistent Agent on Registered Host B will notify FortiNAC of the new adapter. FortiNAC will then remove the adapter from Registered Host A's record and add it to Registered Host B's record. All other adapters associated with Registered Host A remain unaffected.

Example 2: Registered Host A (with Persistent Agent) to Rogue Host B (without Persistent Agent)

Behavior (Default): Adapter remains associated to A when disconnected

When the adapter is disconnected from Registered Host A, FortiNAC is notified that the adapter is offline with Registered Host A. Since Rogue Host B has no way to announce what adapters it owns, the external adapter will remain associated with Registered Host A's record. If the adapter is then connected to Rogue Host B and FortiNAC sees it online, Rogue Host B will be assigned whatever network access policy matches for Registered Host A's record, and the adapter will be shown as online for Registered Host A.

Behavior (requires configuration): Adapter is removed from A when disconnected

Note: Requires CLI configuration - contact Support and reference [KB 193199](#).

Example A: Registered Host A changes network connection

1. Registered Host A disconnects from the external adapter.
2. When Registered Host A changes network connection (e.g. connects to wireless), the agent communicates with FortiNAC and announces the adapters it owns. Since the external adapter is no longer connected, it is not included as one of the adapters. FortiNAC then removes the adapter from Registered Host A's record.
3. Rogue Host B connects using the same external adapter.
4. A Rogue record is created for Rogue Host B and the external adapter is associated.

Example B: Registered Host A is offline when Rogue Host B connects

1. Registered Host A disconnects from the external adapter and remains off the network.
2. Rogue Host B connects using the same external adapter.
3. Since Rogue Host B has no way to announce what adapters it owns, the external adapter will remain associated with Registered Host A's record.
4. After a specific amount of time has lapsed, the "Not Communicating" status is set on Registered Host A's record and the event "Persistent Agent Not Communicating" is generated. The amount of time FortiNAC waits is based upon the value set (in seconds) for "Agent Contact Window on Connect" under **System > Settings > Persistent Agent > Properties** in the Administration UI.

Registered Host A's record will continue to reflect the "Not Communicating" status as long as Registered Host A remains offline and Rogue Host B remains online.

5. When Registered Host A reconnects to the network, the agent communicates with FortiNAC and announces the adapters it owns. Since the external adapter is no longer connected, it is not included as one of the adapters. FortiNAC removes the adapter from Registered Host A's record.
6. If Rogue Host B is online, a Rogue record is created for Rogue Host B with the external adapter associated.

Adapter is moved from a registered host to a rogue

Example 1: Registered Host A (with Persistent Agent) to Rogue Host B (with Persistent Agent):

Once the adapter is removed from Registered Host A and connected to Rogue Host B, the Persistent Agent on Rogue Host B will notify FortiNAC of all adapters (including the new external adapter), and the external adapter will be removed from Host A's host record.

All other adapters associated with Registered Host A remain unaffected.

Example 2: Registered Host A (with Persistent Agent) to Rogue Host B (without Persistent Agent):

When the adapter is disconnected from Registered Host A, FortiNAC is notified that the adapter is offline with Registered Host A. Since Rogue Host B has no way to announce what adapters it owns, the external adapter will remain associated with Registered Host A's record. If the adapter is then connected to Rogue Host B and FortiNAC sees it online, Rogue Host B will be assigned whatever network access policy matches for Registered Host A's record, and the adapter will be shown as online for Registered Host A.

Hosts

Add, delete, modify, locate and manage hosts connected to your network.

The relationship between users, hosts, and adapters is hierarchical. Users own or are associated with one or more hosts. Hosts contain one or more Adapters or network interfaces that connect to the network. By displaying user, host and adapter data in a group, the relationships are maintained. For example, if you search for a host with IP address 192.168.5.105, you are in fact searching for the IP address of the adapter on that host. When the search displays the host, you can click on the Adapters option, the search is automatically re-run and you see the adapter itself. If there is an associated user, you can click on the Users option to re-run the search and see the associated user.

Click on the arrow in the left column to drill-down and display the adapters and their connection status on this host. Hover over the icon in the Status column to display a tooltip with detailed information about this host. For more information, see [Settings on page 216](#). For information on status icons, see [Icons on page 44](#).

The **Displayed** and **Total** fields in the title bar represent the number of records displayed versus the total number of records in the database.



If a host fails one scan and is denied access to the network, but passes another scan at a different time or location and is allowed access to the network, the host will still be marked At Risk because it failed the first scan. The host will continue to be marked At Risk until actions are taken to pass the failed scan.

Navigation, menus, options, and buttons

For information on selecting columns displayed in the Host View Some menu options are not available for all hosts. Options may vary depending on host state.



- Not all options are available when selecting multiple hosts.
- Limit selecting 200 hosts at once.

Field	Definition
Navigation	Across the top of the Hosts View are navigation tools that allow you to quickly move through large numbers of records. These tools include the following: • <<first: Takes you to the first page of records. • <prev: Takes you back one page. • Page Number: Current page number is displayed. • next>: Takes you forward one page. • last>>: Takes you to the last page. • Drop-down Box: Allows you to select the number of records to be displayed on each page.
Quick Search	Enter a single piece of data to quickly display a list of hosts. Search options include: IP address, MAC address, host name, User Name, and user ID. Drop-down arrow on the right is used to create and use custom filters. If you are doing a wild card search for a MAC address you must include colons as separators, such as 00:B6:5*. Without the separators the search option cannot distinguish that it is a MAC address. When quick search is enabled, the word Search appears before the search field. When a custom filter is enabled, Edit appears before the search field.
Right click options	
Add Hosts To Groups	Add the selected host(s) to one or more group(s). See Add hosts to groups on page 231 .
Delete Hosts	Deletes the selected host(s) from the database. Deleting a host from the Host View that is also displayed in the Inventory, removes that host from both views. Deleting a host from the Inventory does not delete it from the Host View. See Delete a host on page 229 .
Disable Hosts	Disables the selected host(s) preventing them from accessing the network. See Enable or disable hosts on page 230 .
Enable Hosts	Enables the selected host(s) if they were previously disabled. Restores network access.
Group Membership	Displays groups in which the selected host is a member. See Group membership on page 231 .
Host Health	Opens a dialog with the contents of the Host Health tab from the Host Properties view. See Host health and scanning on page 224 .
Host Applications	Opens the Applications window for the selected host and lists installed applications. See Application inventory on page 226 .
Host Properties	Opens the Properties window for the selected host. See Properties on page 221 .
Modify Host	Opens the Modify Host window. See Add or modify a host on page 227 .

Field	Definition
Policy Details	Opens the Policy Details window and displays the policies that would apply to the selected host at this time, such as endpoint compliance policies, network access policies, portal policies, or supplicant policies. See Policy details on page 461 .
Register As Device	Changes the selected host to a device in the FortiNAC database. See Register a host as a device on page 232 .
Register As Host	Changes the selected rogue host to a registered host. Displays the Modify Host window. See Add or modify a host on page 227 .
Run Agentless Scan	Manually run an agentless scan for selected hosts. Hosts must be Windows Hosts, members of the domain, have an IP address and be connected to the network.
Scan Hosts	Evaluates the selected host with the scan that applies to the host at that moment. The host must be online and must have a Persistent Agent. If the host is online but does not have a Persistent Agent, it is marked "at risk" for the Scan that most closely matches the host at the moment.
Send Message	Sends a text box message to the selected host(s). The host must be using the Persistent Agent or Mobile Agent. See Send a message to a host on page 233 .
Set Host Expiration	Launches a tool to set the date and time for the selected host(s) to age out of the database. See Set host expiration date on page 233 .
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746.  You must have permission to view the admin auditing log. See Add an administrator profile on page 139.
Set Host Role	Assigns a role to the selected host.
Show Events	Displays the events for the selected host.
Show Network Sessions	View the list of sessions on the host. For more information, see Network sessions on page 274 .
Update Persistent Agent	Opens a dialog that allows you to update the Persistent Agent for the selected host.
Go To Logged On User(s)	Opens the Users tab and displays the users currently logged onto the selected hosts. The logged on user may not be the registered user for the selected host.
Set Logged On User Expiration	Launches a tool to set the date and time for the user currently logged on to the selected host to age out of the database. See Set user expiration date on page 208 .
Set Logged On User Role	Assigns a role to the user currently logged on to the selected host. See Roles on page 620 .
Go To Registered User(s)	Opens the Users tab and displays the registered users for the selected hosts.
Set Registered User Expiration	Launches a tool to set the date and time for the registered user for the selected host to age out of the database. See Set user expiration date on page 208 .

Field	Definition
Set Registered User Role	Assigns a role to the registered user for the selected host. See Roles on page 620 .
Collapse All	Collapses all host records that have been expanded.
Expand Selected	Expands selected host records to display adapter information.
Buttons	
Import/Export	Use Import and Export options to import hosts into the database from a CSV file or export a list of selected hosts to CSV, Excel, PDF, or RTF formats. See Import hosts, users or devices on page 102 or Export data on page 116 .
Options	Displays the same series of menu picks displayed when the right-mouse button is clicked on a selected host.

Settings

The fields listed in the table below are displayed in columns on the Host View based on the selections you make in the Settings window. These fields are also used in custom filters to search for hosts. See [Quick search on page 36](#). Additional fields that can be displayed on the Host View are fields for the user associated with the selected host. See [Search settings on page 199](#).

You may not have access to all of the fields listed in this table. Access depends on the type of license key installed and which features are enabled in that license.

Field	Definition
Agent Platform	Distinguishes between Windows, macOS, iOS, and Mobile Agent.
Agent Version	The version number of the Persistent Agent, Mobile Agent, or Dissolvable Agent installed on the host. None is displayed if the host is a type set to by-pass the agent scan in the endpoint compliance configuration.
Allowed Hosts	The number of hosts that can be associated with or registered to this user and connect to the network. There are two ways to reach this total. If the host is scanned by an agent or if adapters have been manually associated with hosts, then a single host with up to five adapters counts as one host. If the host is not scanned by an agent or if the adapters have not been associated with specific hosts, then each adapter is counted individually as a host. In this scenario one host with two network adapters would be counted as two hosts. Numbers entered in this field override the default setting in System > Settings > Network Device . Blank indicates that the default is used. See Network device on page 910 . If an administrator exceeds the number of hosts when registering a host to a user, a warning message is displayed indicating that the number of Allowed Hosts has been incremented and the additional hosts are registered to the user.
Applications	Applications running on the host. Categories of applications include: antivirus, Hotfixes and operating system.

Field	Definition
Asset Tag	The Asset Tag of the host that is populated by the agent when the asset tag is readable by the agent. The asset tag is derived from the System Management BIOS (SMBIOS).
Authenticated	Indicates whether the host is authenticated.
Delete Hosts When User Expires	If set to Yes, hosts registered to the user are deleted when the user ages out of the database. To modify click Set .
Device ID	If SNMP settings for a device are configured in Account Settings, Device ID can be displayed.
Device Location	If SNMP settings for a device are configured in Account Settings, Device Location can be retrieved and displayed on Users & Hosts > Host page ONLY from public IP.
Device Type	If the Host is a pingable device that is being managed in Hosts view, this field indicates the specific type of device. The Device Type column on the Host page now displays classifications from the expanded FortiGuard-based device type list. Devices detected on the network will show updated, more specific type values that align with FortiGuard's category/subcategory mapping.
Container (Inventory)	Indicates whether this host is also displayed in the Inventory and shows the Container in which it is stored.
Firmware Version	If SNMP settings for a device are configured in Account Settings, Firmware Version of the device can be displayed
First Name	User's first name.
Last Name	User's last name.
Email	User's email address.
Address	User's physical address.
City	User's city.
State	User's state.
Postal Code	User's postal code.
Phone	User's phone number.
Mobile Phone	User's cell phone number.
Mobile Provider	User's mobile provider.
Notes	Notes entered by the administrator. If this user registered as a guest, this section also contains information gathered at registration that does not have designated database fields, such as Person Visiting or Reason for Visit.
Include IP Phones	Appears when any option except Rogue is in the Host Type drop-down list. When selected, hosts that are IP Phones are included in the Host View.
Hardware Type	Type of Hardware, such as a PC.
Created Date	Date the host record was created in the database. Options include last, between, before, and after.

Field	Definition
Expiration Date	Controls the number of days a Host is authorized on the network. Options include Next, Before, After, Between, Never, and None. Host is deleted from the database when the date specified here has passed. The date is automatically calculated based on the information entered when Aging is configured. See Aging out host or user records on page 241 .
Inactivity Date	Controls the number of days a Host is authorized on the network. Options include Next, Before, After, Between, Never, and None. Host is deleted from the database when the date specified here has passed. The date is continuously recalculated based on the information entered in the Days Inactive field. See Aging out host or user records on page 241 .
Last Connected	Date and time of the last communication with the Host. Options include Last, Before, After, Between, and Never.
Endpoint Compliance Scan Status	Display the host status with Passed/Failed/Warning/Not scanned for the Endpoint Compliance scan. (The feature only applies to FortiNAC 7.6.2 and above)
Last Endpoint Compliance Scan	Filter hosts by defining the time/date when last Endpoint Compliance Scan was processed for the host. (The feature only applies to FortiNAC 7.6.2 and above)
Host Name	Name of the host.
Host Notes	Notes about this host.
Host Role	Role assigned to the Host. Roles are attributes of hosts and can be used as filters in a user/host profile. See Roles on page 620. Note: For Microsoft Intune , Host Role represents the Device Ownership of the device managed by Microsoft Intune.
Host Security & Access Value	Value that typically comes from a field in the directory, but can be added manually. This value groups users and can be used as a filter in a user/host profile, which in turn are used to assign endpoint compliance policies, network access policies and Supplicant EasyConnect policies. The data in this field could be a department name, a type of user, a graduation class, a location or anything that distinguishes a group of users. The access value is inherited from the user associated with this host.
Last Modified By	User name of the last user to modify the host.
Last Modified Date	Date and time of the last modification to this host.
Logged On User	Name of the user currently logged into the Host. When machine authentication occurs: FortiNAC will check the previous authentication state of the same host. If the previous authentication was user authentication, the column will be cleared to reflect no user is logged in. When User Authentication occurs: FortiNAC will check and replace previous user information with current authenticated user in the column. If the last authentication was a user authentication, it will always populate the user information.
Managed By MDM/OT	Host is managed by a Mobile Device Management (MDM) or Operational Technology (OT) security system. Data was retrieved from that system for registration. The column will show the MDM/OT Type that managed the host. When hovering over the column, it will show these on a tooltip:

Field	Definition
	MDM/OT Name: The name of the service connector managing the device. MDM/OT Type: The vendor/type of the MDM/OT service connector (e.g., Microsoft Intune, JAMF) In case of Microsoft Intune service connector type, it will also show the Microsoft Intune ID. For unmanaged hosts, the column will not display any info.
MDM/OT Compliant	Host is compliant with MDM or OT policies. This data is retrieved directly from the MDM/OT security system.
MDM Compromised	MDM system has found this host to be compromised, such as jailbroken or rooted.
MDM Data Encryption	MDM system has detected that the host is using data protection.
MDM Passcode	MDM system has detected that the host is locked by a passcode when not in use.
Operating System	Host operating system. This is usually determined based on the DHCP fingerprint of the device or is returned by an agent.
Passed Tests	Shows passed scans.
Persistent Agent	Indicates Persistent agent state with respect to the host. Possible states are: Persistent Agent not installed Persistent Agent installed and communicating Persistent Agent installed and not communicating See Icons for examples.
Registered To	User ID of the user to which this host is registered.
Serial Number	Serial number on the host.
Status	Current or last known status is indicated by an icon. See Icons on page 44. Hover over the icon to display additional details about this Host in a tool tip. • Connected: Indicates whether host is online or offline. • Access: Indicates whether host is enabled or disabled. • Security: Indicates whether host is safe, at risk or pending at risk. • Authentication: Indicates whether or not the user associated with this host has been authenticated. When searching for a host based on Security, search results for Safe include Pending at Risk hosts. Those hosts are a sub-set of Safe hosts. Search results for Pending at Risk do not include Safe hosts.
System UUID	The universal unique identifier used to identify the host.
Title	User's title, this could be a form of address or their title within the organization.
Type	Select the type of host. Host types include: • Rogue: Unknown device that has connected to the network.

Field	Definition
	• Registered Host With Owner: Device that is registered to a known user. Note:The owner is not the same as the logged on user. • Registered Device: Device that is registered by its own host name and is not associated with a single user, such as a library computer or a shared workstation. • Registered Host or Device: Both devices that are registered to users and devices that are registered by host name. • Registered Device In Host View: Pingable device not associated with a user that is managed in the Host View, such as a printer. • Registered Device In Host and Topology: Pingable device not associated with a user that displays in both the Host View and Topology.
User Created	Indicates when this record was created in the database.
User Expires	Controls the number of days a user is authorized on the network. User is deleted from the database when the date specified here has passed. The date is automatically calculated based on the information entered in the Set User Expiration date window. To modify click Set. See Set user expiration date on page 208 for additional information.
User Inactivity Date	Controls the number of days a user is authorized on the network. User is deleted from the database when the date specified here has passed. The date is continuously recalculated based on the number of days entered for Inactivity Limit. For example, if the user logs off the network on August 1st and Inactivity Limit is set to 2 days, the Inactivity Date becomes August 3rd. If on August 2nd the user logs back in again, the Inactivity Date is blank until the next time he logs out. Then the value is recalculated again. To modify click Set.
User Inactivity Limit	Number of days the user must remain continuously inactive to be removed from the database. See Aging out host or user records on page 241 .
User Notes	Notes entered by the administrator. If this user registered as a guest, this section also contains information gathered at registration that does not have designated database fields, such as Person Visiting or Reason for Visit.
User Role	Role assigned to the user. Roles are attributes of users that can be used as filters in user/host profiles. See Roles on page 620 .
User Security And Access Value	Value that typically comes from a field in the directory, but can be added manually. This value can be used as a filter to determine which policy to use when scanning a user's computer. The data in this field could be a department name, a type of user, a graduation class, a location or anything that distinguishes a group of users.
VPN Client	Indicates whether the host connects to the network using a VPN connection.
Vulnerability Details	Displays the specific vulnerability information identified during the scan.
Vulnerability Source	Which vulnerability scanner reported the vulnerability. (Tenable or Qualys)
Vulnerability Scan Status	Indicates whether the scan result meets the configured failure threshold, showing pass or fail accordingly.

Drill-down settings

Use the arrow in the far left column of the Host View to expand a host and view adapter details. Expand or collapse multiple hosts by selecting them and using the right mouse button or **Options**. All adapters associated with a host are contained within the expanded section of the window. Adapters on the same host are considered siblings.

To copy an IP address or physical address, click on the address to highlight it. Press Ctrl+C to copy it.

Settings

Field	Definition
Status	Status of the adapter. Options are Online or Offline and Enabled or Disabled. See Icons on page 44 .
IP address	IP address assigned to the adapter. If the adapter is offline, this is the last known IP address. Supports both IPv4 and IPv6 addresses.
Physical Address	MAC address of the adapter.
Media Type	Indicates whether the adapter is wired or wireless.
Location	The switch and port where the adapter last connected.
Actions	Use the action icons to do the following: • Enable/disable adapter • Access adapter dropneties • Access port properties for the port where the adapter last connected • Go to the Adapters tab and display the adapter for this host

Properties

The Host Properties view provides access to detailed information about a single host. From this view you can access the associated user's properties by clicking on the User option in the menu or the associated adapter's by clicking on the adapter's physical address displayed in the Adapters tab at the bottom of the window.

1. Select **Users & Hosts > Hosts**.
2. Search for the appropriate host.
3. Select the host and either right-click or click **Options**.
4. From the menu select **Host Properties**.

Settings

Field	Definition
General	
Host Name	Name of the host.
Hardware Type	Type of host such as workstation.
Operating System	Operating system installed on the host. Only hosts with a valid operating system can be rescanned. Valid operating systems are Windows, Mac, and Linux.

Field	Definition
Serial Number	Serial number of the host.
Host Status	Radio buttons indicating whether the host is Enabled or Disabled. To enable or disable the host, click the appropriate button and then click Apply.
Time	
Created	Indicates when this host record was created in the database. Options include Before, After, and Between.
Expiration Date	Controls the number of days a host is authorized on the network. Host is deleted from the database when the date specified here has passed. Options include Before, After, Between, Never, and None. If Never is displayed, this indicates that the host will not age out of the database. To modify click Set. See Set host expiration date on page 233 .
Inactivity Date	Controls the number of days a host is authorized on the network. Host is deleted from the database when the date specified here has passed. Options include Before, After, Between, Never, and None. The date is continuously recalculated based on the number of days entered for Inactivity Limit. For example, if the host logs off the network on August 1st and Inactivity Limit is set to 2 days, the Inactivity Date becomes August 3rd. If on August 2nd the host logs back in again, the Inactivity Date is blank until the next time it logs out. Then the value is recalculated again. To modify click Set.
Inactivity Limit	Number of days the host must remain continuously inactive to be removed from the database. See Aging out host or user records on page 241 .
Last Connected	Time the host connection changed to the current connection status. Example: 1. Online host shows Last Connected = 1:00pm 2. Host disconnects from network and FortiNAC changes the host record status to "offline" at 1:20pm 3. Last Connected value updates to 1:20pm 4. Host reconnects to the network and FortiNAC changes the host record status to "online" at 3:00pm 5. Last Connected value updates to 3:00pm
Policy Agent/access	
Role	Role assigned to the host. Use the drop-down list to select a new role.
Agent Version	The version number of the Persistent Agent or Dissolvable Agent installed on the host.
 "None" is displayed if the host is part of a group with an endpoint compliance policy set to by-pass the agent scan.	

Field	Definition
Update Button	Button only displays if the Persistent Agent is installed. Allows you to update this host to a different version of the Persistent Agent.
Security And Access Attribute Value	The value of the attribute that can be used as a filter in user/host profiles. Data for this field can come from a guest template, can be entered automatically from an LDAP directory based on attribute mappings or manually by typing a value in this field. If entered from a directory, the data is copied from the user record of the associated user. For example, if you have a policy for staff and a separate policy for executives, you could enter the word staff for each staff member and executive for each member of the executive group. Enter a matching word on the appropriate user/host profile to match the host to an endpoint compliance or network access policy. See Policy & Objects on page 457 .
Tabs	
Adapters	Displays a list of adapters on this host by MAC address. Click on a MAC address to open the Adapter Properties.
Applications	Displays a list of applications installed on the device. This information is provided by the agent. Typically includes antivirus, Hotfixes and operating system. This information is updated with each successful scan.
Notes	Notes entered by the administrator. If this host is the registered host for a guest, this section also contains information gathered at registration that does not have designated database fields, such as Person Visiting or Reason for Visit.
Health	Lists all the Scans and System scripts, and Administrative states for which the host has been scanned or had applied. Each scan the host is eligible for is shown along with the Name, Status, and Action. Click Show History for short-term historical data. See Host health and scanning on page 224 .
Patch Management	Displays information on patches that have been applied to the host by its associated patch management server. The patch management vendor name and the ID number of the most recent patch is displayed.
Logged In Users	User name of the user logged into this host.
Buttons	
Send Message	Opens the Send Message window and allows you to send a message to a host. If the host has the Persistent Agent or Mobile Agent installed, the message can be sent to the host desktop.  For more details see Send a message to a host on page 233.
Groups	Displays a list of available host groups. If the host is a member of a group the check box is selected. You may add or remove the host from one or more groups.
Apply	Saves changes to the host properties.

Field	Definition
Reset	Resets the values in the host properties window to their previous settings. This option is only available if you have not clicked Apply .

Host health and scanning

Host health is determined by the endpoint compliance policies, system and administrative states, or scans run on the host. Each time a scan is run a record of that scan is stored in the database and displayed on the **Health** tab of the **Host Properties** window. Each scan and scan type the host is eligible for is shown along with the name, status, and action. The agent scan shown in bold text and highlighted with a gray bar indicates the scan that is currently applied to the host. Click **Show History** for short-term historical data.

Scan Configuration Changes

Changes made to a scan configuration only affect the hosts that fail the scan after the change is made. Any hosts that failed the scan prior to the change are not affected. The host must pass the scan before it can take on another host state.

Examples:

- If Host A is scanned, fails Scan A and is assigned a delay of 2 days, changing Scan A to a delay of 5 days does not alter the delay for Host A. It remains 2 days.
- If Host A is scanned, fails Scan A and is marked "At Risk", changing Scan A to Delayed Remediation does not alter Host A. It remains "At Risk" until it passes Scan A.

Multiple Scans Applying to a Host

When multiple scans exist in a host record in Host Health, the combination of the Status fields can affect the host state. If the scan associated with the policy is changed, the results of the original scan are no longer in affect. The endpoint compliance policy that applies to the host now uses a different scan. Failing an Admin or System Scan; however, are still in affect. Refer to the table below for the effects of the Status fields on network access.

Scan type/status				Network access
Admin	System	Agent scan A	Agent scan B*	
Initial	Initial	Failure	Initial	No. Must pass scan B.
Initial	Initial	Failure	Success	Yes
Failure	Initial	Failure	Success	No. Must pass Admin Scan.
Success	Failure	Failure	Success	No. Must pass System Scan.
Success	Success	Failure	Success	Yes

*Agent Scan B is the scan that currently applies to the host in the example in the table.

Access the health tab

1. Select **Users & Hosts > Hosts**.
2. Search for the appropriate host.
3. Select the host and either right-click or click **Options**.
4. From the menu select **Host Properties**.
5. Click on the **Health** tab.

Settings

Option	Description
Type	Admin: Indicates the reason why a host was manually marked at risk. They are not actually scanning the host but provide a configuration or profile with which to associate the host state. Admin Scans can be used to mark hosts At Risk or Safe based on an alarm action triggered by an event. These scans can also be used to enable or disable access based on the time of day, for example to limit access for guests after 5:00 pm. System: These scans run scripts on the FortiNAC platform. Agent: Scans run by an agent installed on the host based on an endpoint compliance policy or set of requirements with which the host must comply. The Agent scan listed in bold and highlighted by a gray bar indicates the scan that is currently applied to the host.
Name	The Name of the scan. There may be more than one scan of a particular type that the host is eligible to be scanned against.
Status	Initial: Default setting indicating that the host has not been scanned, therefore it has neither passed nor failed. For Admin scans, manually setting the scan to Initial is the equivalent of Success. For other scan types, setting the status to Initial has no effect. Failure: Indicates that the host has failed the scan. This option can also be set manually. When the status is set to Failure the host is marked "At Risk" for the selected scan. Failure Pending: The host has been scanned and failed a scan that has the Delayed Remediation option enabled. The host is not placed in remediation and it is marked "Pending At Risk". See Delayed remediation on page 546 for additional information. Success: Indicates that the host has passed the scan. This option can also be set manually. When the status is set to Success the host is marked "Safe" for the selected scan.
Actions	ReScan appears in the Actions column for Agent scans. Clicking ReScan places the host into the queue to be re-scanned. If FortiNAC cannot contact the host when ReScan is clicked, a message is displayed indicating that the host was not rescanned.

View history

1. On the Host Properties Health tab, click **Show History**.
2. View the list of scans, results, and when the scan(s) were performed. Results are sorted with the most recent at the top of the list. Note that if there are no Admin, System, or endpoint compliance policy scan results to display when you click History, the History window opens with the message, "There are no scan results for this host."

3. Inside the History window, click the **Script/Profile name** to view the details of the scan. The details view opens in a new browser window.
4. Close the scan details window.
5. Click **Refresh** on the History view to refresh the list with the most recent data.
6. Close the window when finished.

Application inventory

Application Inventory lists all of the programs found on a selected host either by a FortiNAC Windows, MAC, Linux, or Mobile Agent or an agent from an MDM Service that is integrated with FortiNAC.

Right-click a host in the Host View and select **Host Applications**.



The application inventory is not populated during the initial scan. Subsequent manual or scheduled scans will perform this function.



FortiNAC agents must be version 3.1 or higher to collect application data.

Settings

Field	Definition
Threat Score	The threat score assigned to the application.  This field appears only when the Security Incidents license is enabled.
Operating System	Device operating system, such as iOS.
Operating System Version	The operating system version for the device. (This information may not be available.)
Source	Source of the application data, such as an MDM Service.
Version	Operating system version.
Threat Override	Indicates whether an application as Trusted or Untrusted according to the threat score.  This field appears only when the Security Incidents license is enabled.

Field	Definition
Package Name	The namespace in which the application is run. (This information may not be available.)
Submit Date	The date when the application was last submitted to a Threat Analysis Engine.
	 This field appears only when the Security Incidents license is enabled.
Host Count	The number of hosts that have the application.
Learned Time	Date and time that FortiNAC first learned about this device.
Last Updated	Date and time of the last update t this device in FortiNAC.
Name	Name of the installed application.
Vendor	Domain name of the application vendor.
Version	Version number of the installed application.
Learned Time	Date and time that FortiNAC first learned about this application.
Set Threat Override	Marks an application as Trusted or Untrusted, overriding the existing threat score. The original threat score is not changed, and the override may be set back to "none". Users can also right-click in the Applications table to access this option.
	 This field appears only when the Security Incidents license is enabled.

Add or modify a host

Hosts records are created as hosts connect to the network and register. Hosts can be added by importing or by entering the data manually. See [Import hosts, users or devices on page 102](#). Add or modify host allows you to create new hosts or edit existing ones. Hosts added through this process are either registered to a user or registered as a device.

Register host to user

A host registered to a user is associated with that user, inherits network access parameters from the user and contributes to the **Allowed Hosts** count for the user. Each registered device or host consumes one license when it is online. If the host is registered here, the user will not have to go through the registration process elsewhere, such as the captive portal.

Only hosts with a valid operating system can be rescanned. Valid operating systems are Windows or macOS.

Register host as device

A host registered as a device can be displayed in the Host View or both the Host View and Inventory. This type of host consumes license only when it is online. Typically hosts registered as devices are items such as IP phones, security

cameras, alarm systems or printers.

Add or modify host

1. Select **Users & Hosts > Hosts**.
2. Click **Add**.
3. To modify an existing host, use the search or filter mechanisms on the Host View to locate the appropriate host.
4. Click on the host to select it.
5. Click **Modify**.
6. See the table below for detailed information on each field.
7. Click **OK** to save your data.

Settings

Field	Definitions
Register host to user	
User ID	ID of the user who owns this host. As you type a list of matching user IDs drops down. For example if you type ab, user IDs that start with ab are displayed. If the user ID does not exist in the database, but does exist in the directory used to authenticate users, the user is created at the same time. If the user does not exist either in the directory or in your database, you cannot save the host. If registering this host to a User exceeds the number of Allowed Hosts for that user, a message is displayed indicating that Allowed Hosts has been automatically incremented and the host is registered to the user.
Register host as device	
Create In	Indicates where the device should be displayed. Options include Host view or Host view and Inventory .
Container	If the host is created in both Host View and Inventory, you must choose a Inventory container to contain the host. Containers in Inventory are used to group devices.
General	
Role	Roles are attributes of hosts and users that can be used as filters in user/host profiles. If the host is registered to a user, there are two options for selecting the host role. Use Role From User: Indicates that the host role is inherited from the registered user associated with the host. Specify Role: Indicates that the host role is manually selected. This enables a drop-down list of possible roles from which you can choose. If the host is registered as a device in Inventory only, its role is used to control network access or can be used to apply a CLI configuration. For example, a CLI configuration could be used to reduce the baud rate of a device when it connects to the network.
Host Name	Name of the host being registered.
Hardware Type	Type of hardware such as Printer, Server or Workstation.

Field	Definitions
Serial Number	Serial number on the device. May be of assistance if the device is ever stolen.
Operating System	Operating system on the host.
	 Only hosts with a valid operating system can be rescanned. Valid operating systems are Windows, macOS, and Linux.
Device Type	Indicates the type of device being registered. When registering a host to a user this field defaults to Registered Host With Owner. It could also be set to a gaming or mobile device. When registering as a device, this might be set to devices that are not typically associated with an owner, such as a printer or an alarm system. An icon representing the device selected displays beside the Device Type field. If the device is an Access Point and you register it in Host View, it is removed from the Host View and moved to Inventory after the first poll. It is also removed from the Concurrent License count once it is recognized as an Access Point.
Notes	Free form notes entered by the Administrator.
Security and Access Attribute Value	This value can be included in a filter when determining the Security Policy that should scan this host when it connects to the network. If a directory is in use and a user is associated with this host, the value comes from the directory when it is synchronized with the database. Otherwise the value can be entered manually.
Adapters	Lists the adapters or network interfaces that exist on this host. By listing all adapter's on the host here, you establish that these adapters are siblings. Number of adapters per host is limited to five. See Edit Adapters below. Physical Address: MAC address of the adapter Media Type: Indicates whether the adapter is wired or wireless.

Edit adapters

1. Go to the **Adapter** section of the **Add or Modify Host Window**.
2. **To add an adapter:** Click **Add** and provide the **Physical Address** and the **Media Type**, such as wired or wireless.
3. **To modify an adapter:** Select an **Adapter** and click **Modify**. Change the **Media Type** as needed. To change the **Physical Address** you must delete the adapter and add it again.
4. **To delete an adapter:** Click on the **Adapter** to select it and click **Delete**.
5. Click **OK** to save.



The number of adapters per host is limited to five.

Delete a host

This option deletes the selected host(s) from the Host View.



Deleting a host from the Host View that is also displayed in the Inventory, removes that host from both views. Deleting a host from the Inventory does not delete it from the Host View.



If a device has been detected as a Rogue host and then later manually entered as a device, the Rogue host record remains in the database. It is important to remove the corresponding Rogue host record so there is no conflict between the two records with the same MAC address.

1. Select **Users & Hosts > Hosts**.
2. Use the **Quick Search** or **Custom Filter** to locate the appropriate host(s).
3. Select the hosts to be deleted.
4. Click **Delete**.

Enable or disable hosts

Use this option to disable or enable hosts. A message window appears indicating the successful disabling or enabling of the host. When a host is disabled all of its adapters are disabled.

1. Select **Users & Hosts > Hosts**.
2. Use the **Quick Search** or **Custom Filter** to locate the appropriate host(s).
3. Select the hosts to be enabled/disabled.
4. Click either **Enable** or **Disable**.



Enabling and disabling hosts can be automated using events and alarm mappings. Specific events, such as Possible Mac address Spoof, can be mapped to an alarm that has the action "Disable Hosts" configured. See [Add or modify alarm mapping on page 787](#).

If Security Incidents is enabled



The Security Incidents license must be enabled in order to use the following option.

When enabling a host that was disabled by a security alarm action, a dialog appears that provides the option to:

- Undo the security alarm on the host, which will also undo the associated actions on the host
- Enable the host while leaving the security alarm and its associated actions on the host.

Do one of the following:

- Click **Yes** to undo the security alarm on the host. This will undo the security alarm and the action(s) associated with the security alarm on the host. The number of actions that were undone is displayed. Secondary tasks are performed on the host, if enabled.
- Click **No** to enable the host but maintain the security alarm. All actions associated with the security alarm will remain on the host.

Add IP phones

IP phones can be added using one of the following methods:

- Import IP Phones using a .csv file. See [Import hosts, users or devices on page 102](#).
- Connect your phones to the network and then convert the rogue hosts to IP phones using the Register As Device tool. See [Register a host as a device on page 232](#).
- Connect your phones to the network and use the device profiler feature to automatically register them as IP Phones. See [Profiled devices on page 251](#).
- Add a new host in the Host View and choose Register As A Device in the Add window, then select IP Phone as the device type. See [Add or modify a host on page 227](#).

For more information, see [Policy details on page 461](#).

Add hosts to groups

You can add selected host(s) to groups you have created. See [Groups on page 843](#) for detailed information on Groups and how they are used in FortiNAC. Only registered hosts can be added to groups.

IP phones have a special group type and can only be added to IP phone groups. If you select IP phones with other registered hosts you will not be allowed to use the **Add Hosts To Groups** option. Select IP phones separately. Only IP phone groups will be displayed.

1. Select **Users & Hosts > Hosts**.
2. To select host(s) with specific parameters use the custom filter to set the criteria.
3. Use Ctrl-click or Shift-click to select the records you wish to add to the group.
4. Right-click and select **Group Membership**.
5. The **Group Membership** view lists the available host groups and sub-groups. Sub-groups are displayed under their parent group or groups.
6. To add the hosts to a group, click the box next to the group name and then click **OK**.
7. To create a missing group:
 - a. Click **Create Group**.
 - b. Enter a group name.
 - c. If the new group should be a sub-group of an existing group, enable the **Parent Group** option and select the appropriate group from the list.
 - d. **Description** is optional.
 - e. Click **OK** to save the new group.
8. Click **OK**.

Group membership

From the Host View, you can view or modify the group membership of an individual host. Use this option to open a window that displays a list of all groups to which the selected host belongs.

IP phones have a special group type and can only be added to IP phone groups. If you select an IP phone only IP Phone groups will be displayed.

1. Select **Users & Hosts > Hosts**.
2. To select host(s) with specific parameters use the custom filter to set the criteria.

3. Click on a host to select it.
4. Right-click or click **Options** and select **Group Membership**. The **Group Membership** option displays only for registered hosts.
5. The **Group Membership** view lists the available host groups and sub-groups. Sub-groups are displayed under their parent group or groups. A check next to a group name indicates that this host is contained in that group.
6. **To add the host to a group**, click the box next to the group name and then click **OK**.
7. **To remove the host from a group**, click to uncheck the box next to the group name and then click **OK**.
8. Click **OK** to save your group selections.

Register a host as a device

Devices such as printers, lab hosts, and servers that have not been placed in the Inventory but are connected to managed switches, are created as rogue hosts. If rogue hosts are denied access to the network, they are disabled. Use this option to prevent rogue hosts from being denied access to the network by registering them.

If you select more than one device on the Host View, the **IP Address** and **Physical Address** fields will not display on the **Register As Device** window. If multiple devices are selected and those devices do not have IP addresses, you will not be able to place them in the Inventory using the **Register As Device** option. You can place those devices in the Host View using the **Register As Device** option.

A host can be registered as a device from the Host View based on the rogue host record or from the **Adapter View** based on the adapter record.

1. Select **Users & Hosts > Hosts** or **Users & Hosts > Adapters**.
2. Use the **Quick Search** or **Custom Filter** to locate the appropriate record.
3. Click the record to select it. Click **Edit**. If in **Users & Hosts > Adapters**, right click the record and select **Edit Host**.
4. Click **Create In** and select where this device should be placed. Options include:
 - **Host View**: device is kept in Host View allowing you to track connection history and can be associated with a user.
 - **Host View and Topology**: device is shown in both the Host View and Inventory. You can track connection history and it can be associated with a user, but it cannot be polled.



If the device is an Access Point and you register it in Host View, it is removed from the Host View and moved to Inventory after the first poll. It is also removed from the Concurrent License count once it is recognized as an Access Point.

5. Click **Device Type** and select a type from the drop-down list. The icon associated with the selected device type displays to the right of the drop-down list.
6. Click **Role** and select a role from the drop-down list. Roles are configured on the **Roles** view. You can also click **Add Role** to add a role. See [Roles on page 620](#).
7. Select the **container** for the device from the drop down list. This is where the device will display in the Inventory. This field is disabled if the device is not being managed in the Inventory.
8. The **Physical Address** field is read-.
9. Click **OK**.

Set host expiration date

The expiration date on a host determines when it is automatically deleted or aged out of the database. Aging out of the database can be triggered by an expiration date, the amount of time the host has been inactive or both. There are many methods for setting an Expiration date. See [Aging out host or user records on page 241](#) for information on other methods.

The Set Host Expiration Date feature is used from the Host View.

1. Select **Users & Hosts > Hosts**.
2. Use the **Quick Search** or **Custom Filter** to locate the appropriate host(s).
3. Select the hosts to be modified.
4. Right-click and select **Set Host Expiration**.
5. Use the table below to enter expiration criteria.
6. Click **OK** to set the expiration dates.

Set Host Expiration Settings

Field	Definition
Set Host Expiration	Enables the expiration date option and corresponding calculation methods.
Specify Date	Allows you to select a specific date that the host will be aged out of the database.
Days Valid From Now	Enter the number of days (integer format) from today that you would like the host to expire.
Days Valid From Creation	This is the number of days (integer format) from the date the host record was created.
No Expiration	This host is never deleted from the database even if global or group aging options are added or modified.
Default Expiration	Defaults to the global aging settings configured in System > Settings > User/ Host Management > Aging .
Set Host Inactivity Limit	Enables the option to delete a host based on the number of days that it did not log onto the network.
Days Inactive	Number of consecutive days (integer format) the host must be inactive to be aged out of the database.
No Inactivity Limit	With this option enabled, the host is never deleted from the database due to inactivity even if global or group aging options are added or modified.
Default Inactivity Limit	Defaults to the global aging settings configured in System > Settings > User/ Host Management > Aging .

Send a message to a host

You can send a text message to the selected host from the Host View.

- If the host is online (connected) the message is sent.
- If the host is offline when the message is sent, by default the message expires immediately. If you set a specific expiration time, the message remains active until either the host comes online or the message lifetime is reached.

- If the message is still active when the host comes online, the message is delivered. Otherwise, the host does not receive the message.
1. Select **Users & Hosts > Hosts**.
 2. Use the **Quick Search** or **Custom Filter** to locate the appropriate host(s).
 3. Click the host(s) to select it. Right-click and select **Send Message**.
 4. Enter the message in the **Message** block.
 5. Optionally, enter a Web Address that will be sent as part of the message.
 6. This web address must include the http:// or ftp:// or other information. The page must also be in a location that the host(s) can access from their VLAN such as Remediation, Quarantine, Dead End, or other. For example, if a host is in Remediation, the web page must be accessible from the Remediation VLAN.
 7. Click the radio button next to the **Message Lifetime** option and enter the required information.

Options	Description
Expires after sending to currently connected users	The message expires immediately after it has been sent.
Expires after	The message expires after the specified amount of time. Enter a number and select the timeframe of Minutes, Days, or Hours. The message remains active on the server for the selected timeframe. The server sends the message the next time it communicates with a host as long as communication occurs before the message expires.
Expires at	The message expires on the specified date and time. The format is MM/DD/YY hh:mm AM/PM. The message remains active on the server until the specified date and time. The server sends the message the next time it communicates with a host as long as communication occurs before the message expires.



The server can only send messages to hosts with which it is communicating that have Persistent Agent or are registered with Mobile Agent.

8. Click **OK**.

Host registration and user authentication

A registered host is a device requiring network services that is displayed in the Host View and has an ID. Registered hosts have a record in the FortiNAC database and are known entities. There are several methods for registering hosts depending on the type of host.

- Users connecting to the network with their computers or with a gaming device, such as an Xbox, typically register their equipment through a web page. See
- Rogue hosts connecting directly to the network, such as an alarm system or a security camera, can be registered automatically using device profiler or manually using the Register as Host or Register as Device options in the Host View. See [Profiled devices on page 251](#), [Add or modify a host on page 227](#) and [Register a host as a device on page 232](#).
- Hosts can be registered by importing their records from a .csv file into the database. See [Import hosts, users or devices on page 102](#) for more information.

Registered hosts have specific icons that represent the type of device or host that has been registered and their last known state. See [Icons on page 44](#) for a list of icons and their definitions.

If gaming devices are registered, they are automatically placed in the forced scan exceptions and forced authentication exceptions groups. This prevents them from being scanned or forced to authenticate when they are on the network.

An authenticated user is a network user that has entered a user name and password on a login page and been verified using an existing authentication method. Authentication methods include the local FortiNAC database, an LDAP directory, a RADIUS server or a combination in which a user is authenticated by a RADIUS server and registered using data in LDAP. An authenticated user has a specific icon in the user view that is separate from the icon representing their computer on the Host View.

A single computer can have more than one icon if it has more than one network interface. For example, if a user has a laptop computer with both wired and wireless access to the network, there will be several records and icons for that user and host combination:

- One record in the user view for the user
- One record in the Host View for the computer itself
- Two records in the adapter view for the wired and wireless adapters

The two adapters are called siblings because they reside on the same computer. If the host is disabled by FortiNAC both adapters are automatically disabled also. Adapters can be disabled individually if they are disabled manually.

Important: FortiNAC is only able to associate multiple adapters to the same host when an agent is run on the computer. The agent reports to FortiNAC the MAC addresses of each adapter enabled at that time. Otherwise, FortiNAC creates a separate host record for each adapter record.

Using the previous example, the following would be created when not using an agent :

- One record in the user view for the user
- Two records in the Host View for the computer (one associated with the wired adapter and one to the wireless)
- Two records in the adapter view for the wired and wireless adapters

Registration process

FortiNAC uses the host registration process to create registered hosts in its database. A registered host is a known entity that has an ID. Hosts can be computers, gaming devices, IP phones or any device that requires network services.

Existing host

A host attempts to connect to the network.

FortiNAC compares the host information with the host records in its database.

If the host record exists and has not been disabled, FortiNAC allows access to the network.

New host - captive portal

If the host record does not exist, a Registration web page is displayed, forcing the user to register the equipment.

The user selects the type of registration, such as guest, network user or gaming device.

On the next page, the user enters a user name and password. This provides identity for the computer or gaming device being registered.

If a computer is being registered, the security policy for this user may require that the user download an agent to scan the computer. See [Determining host operating system on page 534](#).

When the computer has met all of the criteria of the scan, it is registered and allowed access to the network.

New host - Passive Agent registration

When a user logs onto or off of the network a Passive Agent is served to the user's computer.

The computer is scanned and registered. See [Passive Agent on page 604](#).

Registration logs

FortiNAC generates a log entry for each host that registers. A new log file is created for each day. The log is a delimited text file. The file is stored in the `/home/cm/registration` directory. The file name is `RegistrationLog.mm.dd.yyyy`, such as `RegistrationLog.03.15.2009`. The record for each host contains the following information:

Settings

Data	Description
First Name	User's first name as entered on the Registration page.
Last Name	User's last name as entered on the Registration page.
Login	User's login for the network.
Hardware Type	User's hardware type; for example, wired, wireless.
Location	Hardware's location on your network.
IP address	The IP address assigned to the hardware's location.
Physical Address	MAC address of the hardware.
E-Mail	The e-mail address to be used to contact the user.
Position/Grade	The position of the user; for example, Professor, or Administration. Or, the grade of the student; for example, year of graduation.
Address	User Contact information.
City	
State	
Zip/Postal Code	
Phone	
PC Name	The name of the PC.
PC Type	The type of the PC; for example, a server, laptop or desktop.
PC Serial Number	The serial number of the PC.
Registration Date/Time	The date and time the user and equipment were registered. The format is MM.DD.YYY HH:MM:SS AM(PM); for example: 09.05.2008 09:45:33 AM

Adapter View

Adapter View is part of a window that includes menu options for users, adapters, hosts, and applications. Use the adapter view to locate and manage adapters connected to your network.

The relationship between users, hosts, and adapters is hierarchical. Users own or are associated with one or more hosts. Hosts contain one or more Adapters or network interfaces that connect to the network. By displaying User, Host and Adapter data in a group, the relationships are maintained. For example, if you search for a host with IP address 192.168.5.105, you are in fact searching for the IP address of the adapter on that host. When the search displays the host, you can click on the Adapters option, the search is automatically re-run and you see the adapter itself. If there is an associated user, you can click on the Users option to re-run the search and see the associated user.

Hover over the icon in the **Status** column to display a tooltip with detailed information about this adapter. For settings, see [View and search settings on page 239](#). For information on status icons, see the [Icons on page 44](#).

The **Displayed** and **Total** fields in the title bar represent the number of records displayed versus the total number of records in the database.

Navigation, menus, options, and buttons

Some menu options are not available for all adapters. Options may vary depending on adapter state.

Double-click on an adapter to display adapter properties.

Field	Definition
Navigation	Across the top of the Adapters tab are navigation tools that allow you to quickly move through large numbers of records. These tools include the following: • <<first: Takes you to the first page of records. • <prev: Takes you back one page. • Page Number: Current page number is displayed. • next>: Takes you forward one page. • last>>: Takes you to the last page. • Drop-down Box: Allows you to select the number of records to be displayed on each page.
Quick Search	Enter a single piece of data to quickly display a list of adapters. Search options include: IP address, MAC address, host name, User Name, and user ID. Drop-down arrow on the right is used to create and use custom filters. If you are doing a wild card search for a MAC address you must include colons as separators, such as 00:B6:5*. Without the separators the search option cannot distinguish that it is a MAC address. When Quick Search is enabled, the word Search appears before the search field. When a custom filter is enabled, Edit appears before the search field.
Right click options	
Adapter Properties	Opens the Properties window for the selected adapter. See Properties on page 240 .
Disable Adapters	Disables the selected adapter(s) preventing them from accessing the network. See Enable or disable an adapter on page 241 .
Enable Adapters	Enables the selected adapter(s) if they were previously disabled. Restores network access.

Field	Definition
Modify Adapter	Opens the Modify Adapter window for the selected adapter. See Modify an adapter on page 241 .
Add To Docking Station Management	Add the unauthenticated host/device from the Docking Station Connected column as a trusted host. The host MAC address will be listed as a trusted host/device in Docking Station Management.
Port Properties	Opens Port Properties for the port where the selected adapter is connected. See Port properties on page 360 .
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746 .
	 You must have permission to view the admin auditing log. See Add an administrator profile on page 139.
Enable Hosts	Enables the host(s) associated with the selected adapter(s) if they were previously disabled. Restores network access.
Disable Hosts	Disables the host(s) associated with the selected adapter(s) and all of its other adapters preventing them from accessing the network. See Enable or disable an adapter on page 241 .
Host Health	Opens a dialog with the contents of the Host Health tab from the Host Properties view. See Host health and scanning on page 224 .
Host Applications	Opens the Applications window for the selected host and lists installed applications. See Application inventory on page 226 .
Go To Host(s)	Opens the Hosts tab and displays the hosts associated with the selected adapters.
Show Network Sessions	View the list of sessions on the adapter. For more information, see Network sessions on page 274 .
Modify Host	Opens the Modify Host window for the host associated with the selected adapter. Applies only to registered hosts.
Register As Device	Changes the host associated with the selected adapter to a device in the FortiNAC database. See Register a host as a device on page 232 .
Register As Host	Changes the Rogue host associated with the selected adapter to a registered host. Displays the Modify Host window. See Add or modify a host on page 227 .
Scan Hosts	Scans the associated host with the Security Policy that applies to the host at that moment. The host must be online and must have a Persistent Agent. If the host is online but does not have a Persistent Agent, it is marked "at risk" for the Security Policy that most closely matches the host at the moment.
Run NMAP Scan	Determines open ports and operating systems on the device being scanned
Send Message	Sends a text box message to the associated host(s). User can send messages to hosts with the Persistent Agent or Mobile Agent installed. See Send a message to a host on page 233 .

Field	Definition
Set Host Expiration	Launches a tool to set the date and time for the associated host(s) to age out of the database. See Set host expiration date on page 233 .
Set Host Role	Assigns a role to the associated host.
Create Device Profiling Rule	Displays the Add Device Profiling Rule dialog with some information pre populated from the selected Adapter.
Test Device Profiling Rule	Ability to test an adapter against a DPC Rule to see if it matches or not Note: Test uses data currently stored in the database (such as IP address information) and does not attempt to update this information prior to running the test.
Go To User(s)	Opens the Users tab and displays the users associated with the selected adapters.
Set User Expiration	Launches a tool to set the date and time for the user associated with the selected adapter to age out of the database. See Set user expiration date on page 208 .
Reprofile Rogue(s)	Ability to run DPC rules against one or more rogues selected.
Set User Role	Assigns a role to the user associated with the selected adapter. See Roles on page 620 .
Buttons	
Import/Export	Use Import and Export options to import hosts into the database from a CSV file or export a list of selected hosts to CSV, Excel, PDF, or RTF formats. See Import hosts, users or devices on page 102 or Export data on page 116 .
Options	Displays the same series of menu picks displayed when the right-mouse button is clicked on a selected host.

View and search settings

The fields listed in the table below are displayed in columns on the **Adapter View** based on the selections you make in the Settings window. These fields are also used in custom filters to search for adapters. See [Quick search on page 36](#). Additional fields that can be displayed on the **Adapter View** are fields for the user or the host associated with the selected adapter.

Settings

Field	Definition
Access Value	Name or number of the network access identifier given to this adapter based on the state of the host and the device to which the adapter is connected, such as VLAN ID, VLAN Name or Aruba Role.
Description	Free form notes entered by the Administrator about this adapter.
Device Type	This field displays device type classifications from the expanded FortiGuard-based device type list. Devices detected on the network will show updated, more specific type values that align with FortiGuard's category/subcategory mapping.

Field	Definition
IP address	The primary IP address assigned to this adapter that is used to communicate with FortiNAC. If the adapter is offline, this is the last known IP address for the adapter. Supports both IPv4 and IPv6 addresses.
All IPs	All IP addresses assigned to the adapter. Supports both IPv4 and IPv6 addresses. - For IPv6, all addresses used for IPv6 communication will be displayed. - For IPv4, IP addresses used for registration, remediation, isolation, etc., will be displayed along with the production IP until a L3 poll determines the single IP being used. - Depending on the ARP cache aging of the L3 device itself and the poll interval that FortiNAC polls it, multiple production IP addresses may be displayed simultaneously for an adapter.
Location	Name of the switch and port where this adapter is connected to the network. If the adapter is offline, this is the last known location where the adapter connected to the network.
Media Type	Indicates whether this is a wired or wireless adapter.
Physical Address	MAC address of the adapter.
Status	Current or last known status is indicated by an icon, see Icons on page 44 . Hover over the icon to display additional details about this adapter in a tool tip. Connected: Indicates whether host is online or offline. Access: Indicates whether host is enabled or disabled. Valid Physical Address: Indicates whether or not the system knows the MAC address for the adapter that has connected to the network.
Vendor Name	Name of the vendor that matches the vendor OUI for this device.

Properties

The Adapter Properties view provides access to detailed information about a single adapter. From this view you can access the associated user's properties by clicking on the User tab or the associated host by clicking on the Host tab. Adapter properties also provides access to the Device Identity tab. See [Endpoint Fingerprints on page 245](#).

1. Select **Users & Hosts > Adapters**.
2. Search for the appropriate adapter.
3. Select the adapter and either right-click.
4. From the menu, select **Adapter Properties**.

Settings

Field	Description
IP address	IP address assigned to the adapter. This field displays the last known IP address until a new one is found. If the adapter no longer has an IP address, the last known IP will continue to display.

Field	Description
Physical Address	MAC address of the adapter.
Location	Switch and port where the adapter is connected to the network.
Media Type	Indicates whether this is a wired or wireless adapter.
Adapter Status	Radio buttons indicating whether the adapter is Enabled or Disabled. To enable or disable the adapter, click the appropriate button and then click Apply.
Description	Free form notes section for the administrator.
Apply	Saves changes to the adapter properties.
Reset	Resets the values in the Adapter Properties window to their previous settings. This option is only available if you have not clicked Apply.

Enable or disable an adapter

Use this option to disable or enable adapters. A message window appears indicating the successful disabling or enabling of the selected adapters. If a host has more than one adapter, only the selected adapter is disabled.

1. Select **Users & Hosts > Adapters**.
2. Use the **Quick Search** or **Custom Filter** to locate the appropriate adapter(s).
3. Select the adapters to be enabled/disabled.
4. Click either **Enable** or **Disable** at the bottom of the **Adapter View**.

Modify an adapter

1. Select **Users & Hosts > Adapters**.
2. Search for the appropriate adapter.
3. Select the adapter and either right-click and select **Edit** or click **Edit** at the top of the view.
4. The **Physical Address** field cannot be modified.
5. Click in the **Media Type** field and select either **Wired**, **Wireless** or **Unknown**.
6. In the **Description** field, enter any notes on this adapter.
7. Click **OK** to save your changes.

Aging out host or user records

Host and User records remain in the database indefinitely unless you set expiration dates for those records. There are several methods for setting expiration dates.

As new hosts, users or administrators are added to the database, the **Expiration Date** and/or **Inactivity Date** are automatically populated based on settings elsewhere in FortiNAC. Aging settings are configured using the methods listed below. If no global settings have been established and hosts or users are added without Expiration or Inactivity dates, those dates can be added later by configuring the settings below.

If you set age times for existing users or hosts, you may inadvertently cause them to be deleted from the database. If the expiration date calculated for those hosts or users is before today's date, those records will be removed from the database.

Aging a large number of hosts or users at the same time can cause processing delays with FortiNAC if users attempt to re-register within a short period of time of each other. It is recommended that you stagger the aging times to reduce the number of possible re-registrations at any given time.

Host age times are evaluated every ten minutes. If you specify a date and time, the host may not be removed from the database for up to ten minutes after the time selected.

The user inactivity timer is started when all hosts registered to a user are seen as offline. When a host is seen as connected, the timer is cleared. The timer is also cleared when the user logs into FortiNAC.

Directory	If the Time To Live option is enabled in the Directory Attribute Mappings window, the value stored in the directory is used to calculate the expiration date and inactivity date. This is based on the user's record in the directory. For the user, only the expiration date is calculated. For the host, both the expiration date and the inactivity date are calculated. This may also apply to administrators. The host must be associated with a user to inherit these settings.
System Settings	Age times under System > Settings > User/Host Management > Aging are used to populate Expiration Date and Inactivity Date for hosts as they are added to the database and Expiration Date for Users. If these settings are configured after administrators, network users or hosts have been added to the database, those without age times or that are not set to Never Expire, will be automatically updated. Records with age times are not modified. See Aging on page 1006 .
Group Aging	You can create a host group and use Group Aging to populate the Expiration Date and/or the Inactivity Date fields for hosts in that group. All hosts in the group are modified even if they already have an age time set, except those set to Never Expire. See Aging hosts in a group on page 851 .
Host Aging	You can enter or override aging values for individual hosts by clicking Set on the Host Properties window or using the Set Host Expiration Date option on the Host View. See Set host expiration date on page 233 .
User Aging	You can enter or override those values for individual users, including administrators, by clicking Set on the User Properties window or using the Set User Expiration Date option on the user view. See Set user expiration date on page 208 .
Administrator User Aging	Administrators never age out of the database under any circumstances. These users must be removed from the database manually from the administrators View.
Administrative User Aging	Administrators are treated like regular network users when aging settings are applied, depending on how they are added to the database. Below are ways to set the expiration date for an administrator: • When adding an administrator from the administrator users view, the new user will receive an expiration date based on the information in the global aging settings, the Time To Live setting in the directory or based on a group setting if they are placed in a group. See Aging on page 1006. • Manually give any administrator an expiration date by selecting the user on the administrators View and using the Set Expiration option. See Set user expiration date on page 208.

- When an administrator is added by converting an existing network user to an administrator, the new administrator can have aging set through any of the possible aging options.
- If you assign administrator profiles based on directory groups, there are circumstances in which an administrator would be assigned an expiration date. See [Set privileges based on directory groups on page 149](#).
- If a non-administrator registered a host through the captive portal and a directory synchronization is run, the user would then be converted to an administrator. However, it would have an expiration date based on the global aging settings. This also occurs when a host is registered to a user manually by an administrator.

Guest Aging

A Guest user's expiration date is set based on the Account Duration entered in the guest template used to create the Guest. The host registered to the Guest inherits its expiration date from the Global Aging settings. When the Guest user's account expires, both the Guest user's account and the guest's registered host are automatically removed from the database. If the host's expiration date is earlier than the Guest user's expiration date, the host is removed from the database, but the Guest user account remains.

Application view

The application view is part of a window that includes menu options for users, adapters, hosts, and applications.

Applications for scanned hosts connected to your network appear in the application view. As hosts are scanned, the list of applications is updated.

You may not have access to all of the fields listed in this table. Access depends on the type of license key installed and which features are enabled in that license.

The fields listed in the table below are displayed in columns on the application view based on the selections you make in the Settings window. See [Configure table columns and tooltips on page 197](#). Most of these fields are also used in custom filters.

Settings

Field	Definition
Add Filter	Allows you to select a field from the current view to filter information. Select the field from the drop-down list, and then enter the information you wish to filter. Options include: • Name • OS • OS Version • Package Name • Source • Threat Override. Select Trusted or Untrusted. For Security Incidents only. • Threat Score (Security Incidents only) - Enter a single number or a range of numbers

Field	Definition
	(e.g., 8-10) • Vendor • Version See Filters on page 34 .
Update	Displays the filtered data in the table.
Security events	
Name	The name of the application.
Threat Score	The threat score assigned to the application.  This field appears only when the Security Incidents license is enabled. You must have Security Incidents enabled in your licensing package in order to use Security Incidents features.
Version	The version of the application being scanned. (This information may not be available.)
Vendor	The name of the vendor providing the application. (This information may not be available.)
Operating System	The operating system of the device containing the application.
Operating System Version	The operating system version for the device. (This information may not be available.)
Source	The agent that is used to scan the application.
Threat Override	Indicates whether an application as Trusted or Untrusted according to the threat score. This field appears only when the Security Incidents license is enabled. You must have Security Incidents enabled in your licensing package in order to use Security Incidents features.
Package Name	The namespace in which the application is run. (This information may not be available.)
Submit Date	The date when the application was last submitted to a Threat Analysis Engine.  This field appears only when the Security Incidents license is enabled.
Host Count	The number of hosts that have the application.
Buttons	
Export	The Export option allows you to export a list of selected applications to CSV, Excel, PDF, or RTF formats.
Options	Displays the same series of menu picks displayed when the right-mouse button is clicked on a selected user.

Field	Definition
Show Hosts	Opens the Host View, displaying the host(s) containing the application. Users can also right-click in the Applications table to access this option.
Delete	Deletes the selected application. Users can also right-click in the Applications table to access this option.
Rescan	Rescans the selected application for threat analysis. Users can also right-click in the Applications table to access this option.
	 This field appears only when the Security Incidents license is enabled.
Set Threat Override	Marks an application as Trusted or Untrusted, overriding the existing threat score. The original threat score is not changed, and the override may be set back to "none". Users can also right-click in the Applications table to access this option. This option appears only when the Security Incidents license is enabled. You must have Security Incidents enabled in your licensing package in order to use Security Incidents features.

Show the host(s) containing an application

1. Select **Users & Hosts > Applications**.
2. Select an application in the table and click **Show Hosts**, or right-click an application and select **Show Hosts** from the menu.

The Host View is displayed showing the host(s) that contain the application.

Set the threat override for an application

Set threat override lets users mark an application as trusted or untrusted, overriding the existing threat score. The original threat score is not changed, and the override may be set back to "none".

You must have Security Incidents enabled in your licensing package in order to use Security Incidents features.

1. Select **Users & Hosts > Applications**.
2. Select an application in the table and click **Set Threat Override**, or right-click an application and select **Set Threat Override** from the menu.
3. Select **Trusted** or **Untrusted** from the drop-down menu.
4. Click **OK**.

Endpoint Fingerprints

FortiNAC continuously collects identity records as hosts connect to the network. These records are used to rapidly identify and categorize new devices as they connect to the network. A list of these device identity matches are displayed

on the Endpoint Fingerprint view. A separate record is added every time a new fingerprint is heard for a MAC. For example, if the adapter on a host is moved from a registration VLAN to a production VLAN and as a result requests a new IP address this creates a new record. If two records are displayed for the same MAC and port, but with different OSs, the host is most likely a dual-boot host. This generates the Device Fingerprint Changed event. The information in this topic can be found for each fingerprint.

FortiNAC-OS Requirement: Certain Fingerprint Attributes require access to the applicable protocol to be enabled. The Fingerprint Attributes table below lists which option is required per attribute (if any). See [Open ports](#) for more details.

Information

Field	Definition
Physical Address	MAC address of the device.
Device Type	Indicates the type of hardware detected. This field displays device type classifications from the expanded FortiGuard-based device type list. Devices detected on the network will show updated, more specific type values that align with FortiGuard's category/subcategory mapping.
Operating System	Operating system of the host. If more than one record is displayed with different operating systems, this host may be dual boot.
IP Address	IP address of the device.
Host Name	The name for this host extracted from the DHCP packet.
Vendor	Manufacturer of the host. This is based on the vendor OUI.
Vendor OUI	First 3 octets of a device's Physical Address.
Source	Method used to identify the device. Sources can be ranked through Set Source Rank .
Rule Name	Name of the Device Profiling Rule that was a match for this device.
Device Registered	Specifies whether the device is registered in the FortiNAC Database or is a rogue device. The number of devices registered or rogue will display above the table header.
Last Heard	The last time FortiNAC matched this fingerprint for this host.
Creation Time	The first time FortiNAC matched this fingerprint for this host.

The information displayed on the table can be configured by hovering over the table's header to reveal a settings icon on the left side of the header.

Along the top of the Endpoint Fingerprint view, interactable charts can be displayed for Device Types, Operating System, Vendor, Vendor OUI, and Source. Hovering over the charts will reveal a settings icon at the top left of the view. Clicking it will provide the option to customize the charts. Charts can be reordered by dragging and dropping the chart to its desired location along the top. Selecting a slice of a chart will filter the fingerprints by that attribute. To remove the filter, click the filter icon to the top right of the chart.

Right-Click Options

Option	Description
Delete	Deletes the selected fingerprint(s).
Show Attributes	Displays the Fingerprint Attributes on page 247 information.
Show Adapters	Displays the adapter information associated with the device.
Register as Device	See Register a host as a device on page 232
Confirm Rule	Confirms the device still matches their associated rule.
Enable Host	Enables the host. See Enable or disable hosts on page 230
Disable Host	Disables the host. See Enable or disable hosts on page 230 .
Create Device Profiling Rule	Displays a window to Add a Device Profiling Rule. See Adding a rule on page 264 .
Run FortiGuard IoT Scan	Runs a FortiGuard IoT Scan.
Test Device Profiling Rule	Tests the selected device profiling rule against the selected host(s).

Fingerprint Attributes

Attribute	Description
Active	
OUTPUT	Output of the Nmap command.
PORTS	Open ports discovered during the Nmap scan.
Agent	
FortiNAC-OS "set allowaccess" option: nac-agent	
UUID	UUID for this host.
HWTYPE	Hardware type for this host.
SERIAL	Serial number for this host.
ASSET_TAG	Asset tag for this host.
SSID	Service Set Identifier for this adapter.
BSSID	Basic Service Set Identifier for this adapter.
MEDIA	Media type for this adapter.
IFDESC	Interface Description for this adapter.
OPERSTATUS	The Operational Status for this adapter.
DHCP	
FortiNAC-OS "set allowaccess" option: dhcp	

Attribute	Description
PARAMLIST	Combination of parameters contained in the DHCP packet that allows FortiNAC to infer the operating system for this host.
OPTIONLIST	Displays a list of option numbers from the DHCP packet used to provide information about the host.
VENDORCLASS	Vendor Class Identifier extracted from the DHCP packet. Allows the DHCP server to return specific information based on the host's hardware type.
MSGTYPE	DHCP message type, including • Discover: Host broadcast initial DHCP request for an IP address. • Request : DHCP server has responded. Host requests an IP address from a specific DHCP server. • Passive: Generated when something about the DHCP fingerprint has changed since the last message, such as a different operating system.
FortiGuard	
CONFIDENCE	How confident FortiGuard is in this host classification.
CAT	Category for this host.
SUBCAT	Subcategory for this host.
OS	Operating system for this host.
SUBOS	Sub operating system for this host.
VENDOR	Vendor of this host.
MODEL	Model of this host.
HTTP/HTTPS	
FortiNAC-OS "set allowaccess" option: http and/ or https	
OUTPUT	HTTP(S) response to the web request.
ONVIF	
UUID	Reported UUID from the ONVIF scan.
HWTYPE	Reported hardware type from the ONVIF scan.
OUTPUT	Raw output of the ONVIF scan.
RADIUS	
FortiNAC-OS "set allowaccess" option: radius and/or radius-local	
Calling-Station-Id	Phone number of the user calling
Called-Station-Id	Phone number of the user called
User-Name	Name of the user to be authenticated
NAS-IP-Address	IP address of the NAS originating the Access-Request

Attribute	Description
NAS-Identifier	String identifying the NAS originating the Access-Request
TLS-Client-Cert-Subject-Alt-Name-Upn	TLS Client Certificate Subject Alternative Name
TLS-Client-Cert-Common-Name	TLS Client Certificate Common Name
Fortinet-Vdom-Name	FortiGate Virtual Domain Name
FortiNAC-Deny	
FortiNAC-Nas-Src-Ip	Source IP of the RADIUS Access-Request
Cleartext-Password	
EAP-Type	EAP Type number
EAP-Type-Name	EAP Type name
User-Password	Password used for authentication. If present, will display as ***
Script	
OUTPUT	Raw output of the executed script.
EXITVALUE	Exit value of the executed script.
SNMP	
FortiNAC-OS "set allowaccess" option: snmp	
RESPONSE	Response from querying the requested OID.
OID	Requested OID.
SSH	
FortiNAC-OS "set allowaccess" option: ssh	
OUTPUT	Raw output of the SSH command.
TCP	
PORTS	List of detected open TCP ports.
Telnet	
OUTPUT	Raw output of the Telnet command.
UDP	
PORTS	List of detected open UDP ports.
Vendor OUI	
VENDOR	Vendor Name of the host.
OUI	Vendor OUI of the host.
ALIAS	Vendor Alias for the host.

Attribute	Description
WinRM	
OUTPUT	
Windows Profile	
UUID	UUID for the host.
HWTYPE	Hardware Type for the host.
ASSET_TAG	Asset tag for the host.
SERIAL	Serial number for the host.
SUMMARY	Summary description of the host.
OUTPUT	Raw output.
DOMAIN	Domain the host belongs to.
PRODUCT_TYPE	Product type of the host.

Profiled devices

Device profiler is a mechanism to automatically categorize and control unknown or rogue devices that connect to your network and receive an IP address. This process runs continuously. It scans the host database for rogues with IP addresses and assigns them a device type based on profiles or rules set up in FortiNAC. Device profile rules use information such as operating system and vendor OUI to determine what the connecting device might be. Device profiler is installed with some default rules which can be refined and new rules can be added. You can evaluate uncategorized rogues manually as new rules are added or existing rules are modified.

During an initial installation of FortiNAC this feature increases the speed with which devices are identified. After installation, device profiler provides easy management of new devices as they come online. Devices that are typically identified by device profiler include items such as IP phones, gaming devices, or mobile devices.

After a device has been categorized, the rule used to profile the device is associated with that device. If the device disconnects from the network and later reconnects, device profiler confirms that the device still matches the rule. If the device does not match its associated rule, device profiler can disable the device or notify the administrator by using events and alarms. Rule confirmation is an optional setting. This setting can be applied globally on the rule itself or individually on a profiled device.

To manage device profiler, you have the option of creating administrators known as device managers with an administrator profile that limits their permissions within FortiNAC. Creating additional users with limited permissions to manage new devices frees your regular IT staff to perform other tasks.

How it works

As new, unknown devices connect to the network, device profiler categorizes them and places the devices within FortiNAC based on its device profiling rules. The process is as follows:

1. A device or host connects to the network.
2. FortiNAC learns that something has connected.
3. The Device Identity feature checks for a MAC address. If the MAC address is available, Device Identity compares it to known MAC addresses.
4. If the MAC address is unknown, the device is placed in the host database as a rogue with any additional information available, such as IP address or operating system. The time interval that device profiler waits to resolve a MAC address to an IP address is 30 minutes, thus allowing time for normal IP to MAC polling to occur.
5. If the device has an IP address, device profiler begins to compare the available device information to its device profiling rules. It starts with the rule that is ranked number one and works its way through the list of rules in order by rank until it finds a match to one of the rule's criteria or matching methods. Disabled rules are ignored.
6. A match is determined by a combination of the device type selected on the General Tab for the rule and one or more methods selected on the Methods Tab. For example, if the device type selected is Mobile Device and the Method selected is DHCP fingerprinting, then a hand held device running Windows CE would match this rule. DHCP fingerprinting would determine that the device is using Windows CE which is an operating system that corresponds to a Mobile Device.

However, if the device type selected is Gaming Device and the Method selected is DHCP fingerprinting, then a hand held device running Windows CE would not match this rule because Gaming Devices do not use Windows CE.

Identification methods based on fingerprinting use the FortiNAC fingerprint database which cannot be modified by the user.

The exception to this is the vendor OUI method. This method ignores the device type selected on the General Tab and uses the information selected within the method, such as the OUI, vendor name, vendor alias or Device Type. Multiple entries are allowed, but the device only has to match one item to match the rule.

7. If **Notify Sponsor** is enabled, an email is sent by the FortiNAC server to all Device managers who have permission for devices associated with this rule. Permissions are based on the configuration of the administrator profile attached to the administrator. The email indicates that a new device has been processed.
8. The device is assigned the device type contained within the rule. Unless it is the Catch All rule which has no type. The type assigned by device profiler takes precedence over any type associated with the device's vendor in the FortiNAC database. See [Vendor OUIs on page 898](#).
9. The device is assigned the role contained within the rule. If no role is selected, the device is assigned the NAC Default role. The role assigned by device profiler takes precedence over any role associated with the device's vendor OUI in the FortiNAC database. See [Vendor OUIs on page 898](#).
10. Devices can be registered automatically or manually. If the rule is set to register manually, you must go to the Profiled Devices window to register the device.
Concurrent license count has been exceeded: New hosts matching a rule will be listed in the Profiled Devices window and will not register. Once the license count is within proper levels, register using one of the following methods:
 - Manually: Right-click and select Register As Device.or
 - Automatically (Rule set to Register: Automatic): Delete the host and allow FortiNAC to re-profile and register it.
11. If **Register As** is enabled in the matching rule, the device can be placed in the Host View, or the Inventory, or both.
12. If you choose **Host View**, the device can be added to a specific group as it is added to the Host View.
13. If you choose **Inventory**, the device is added to a user-specified container.
14. If the Access Availability option has been set to Specify Time, network access for devices placed in the Host View is limited to the configured times. To prevent devices from accessing the network outside the configured timeframe, they are marked "At Risk" for the Guest No Access admin scan.
15. When the device has been through the entire process and has been registered either automatically or manually, it will no longer display as a rogue. Depending on the options you chose in the rule it is displayed in the Host View, the Inventory, or both.
16. If the device does not match any rule, it is associated with the default Catch All rule. Depending on the settings configured within this rule, the device can be associated with the rule but still remain a rogue.
17. Devices that are registered and associated with a user are placed in the Host View and removed from the Profiled Devices window. Devices that are placed in Inventory only are removed from Profiled Devices. All other devices processed by device profiler remain in the Profiled Devices window and in the Host View.

Configure profiled devices

The profiled devices view displays a list of devices that have been profiled using the device profiling rules. Based on how closely each device matched a rule it was given a device type and placed either in the Inventory, the Host View, or both. Devices placed in the Inventory do not display on the **Profiled Devices** tab. Devices placed in the Host View are shown on the **Profiled Devices** tab. When a device is registered and it has an associated user, it is removed from the **Profiled Devices** tab and displays only in the Host View.

Administrators can access this list of devices. Device managers can only see those devices that match rules listed in the device manager's profile.

Only administrators with additional permissions have access to the **Views** column, as well as **Rule Settings**, **Confirm Rule**, and **Details** on the **Profiled Devices** view. See [Permissions list on page 133](#) for additional information.

Entries in this window are devices that require network services. Typically they include things such as mobile devices, gaming devices or PCs. They are considered hosts on the network. Only those devices associated with a device profiling rule are displayed.

New devices are not displayed in the **Profiled Devices** view unless you click **Refresh** or close and reopen the tab.

Devices identified by a device profiling rule maintain their association with that rule. If rule confirmation is enabled, the associated rule and the device are checked periodically to see if the rule is still valid for the device. Rule confirmation can be enabled for a rule, which affects all devices associated with the rule, or it can be enabled for individual devices.

Settings

Field	Definition
Rogue Evaluation Queue Size	Indicates the number of rogues waiting to be processed by the device profiling rules. The queue is filled by rogues as they connect to the network. If Run on the Device Profiling Rules window is clicked, any rogues that were not previously categorized are added to the queue immediately. This number will move up and down as the system processes rogues.
Name	Name of the user associated with this device or the name of the manufacturer. For example, if a PC connects and has no associated user, you may see DELL, INC. in the name field. If the device is registered, but has no associated user the name field may be blank. Devices that are registered and have an associated user display in the Host View but are removed from the Profiled Devices tab.
Rule Name	Name of the Device Profiling Rule that was a match for this device.
Type	Icon that represents the type of host, such as Mobile Device or Gaming System. This field is populated by the Device Profiling Rule. Device type can also be assigned by vendor OUI; however, the type in the Device Profiling Rule takes precedence. If this host is associated with a user, a host status icon is displayed. See Icons on page 44 This field displays device type classifications from the expanded FortiGuard-based device type list. Profiled devices will show updated, more specific type values that align with FortiGuard's category/subcategory mapping.
Role	Role assigned to this host by the Device Profiling Rule. Roles can also be assigned by vendor OUI; however, the role in the Device Profiling rule takes precedence.
IP address	IP address of the device.
Physical Address	MAC address of the device.
Location	Location where the device connected to the network.
Notes	Indicates whether or not there are notes for this device.
Registered	Indicates whether or not the device is registered.

Field	Definition
Views	Displays icons for the FortiNAC views that can be accessed for this device. Click an icon to go to the view. Possible views include: Adapter, group membership, port properties and Device Properties.
Confirm Rule On Connect	If enabled, device profiler confirms that previously profiled devices still match their associated rule the next time they connect to the network. A green check mark indicates that the option is enabled. A red circle indicates that the option is disabled.
Confirm Rule Interval	If enabled, displays the interval used to confirm device rules, such as 2 Days. Indicates that device profiler will confirm that the associated rule matches the device every two days.
Last Confirmation Time	If Rule Confirmation is enabled, this column displays the last time this device had its associated rule confirmed.
Confirmation Failure Action	If Rule Confirmation is enabled, this column indicates the action to be taken if a device no longer matches its associated rule. Options are Disable Device or None.
Export	Exports data to a file in the default downloads location. File types include CSV, Excel, PDF, or RTF. See Export data on page 116 .
Right click options	
Register As Device	Registers selected devices. If the device is not associated with a user, the name is blank or displays as ROGUE, ROGUE. If the device is associated with a user, it is removed from the Profiled Devices tab and displays in the Host View.
Delete	Deletes selected devices from the database. This deletes the hosts from both the Profiled Devices window and the Host View.
Rule Settings	Changes rule confirmation settings for the selected device.
Confirm Rule	Runs the rule confirmation process for the selected device. If the device does not match the rule an event is generated. See Events and alarms on page 259 . The device must be online in order to confirm the associated rule.
Details	Allows you to modify the role of a single device. Only available for Administrators users.
Notes	Opens the Notes window for the selected device. Allows you to add a note and view previous notes. Notes include the date and time they were created.
Enable	Enables the selected device.
Disable	Disables the selected device.

Export profiled devices

This option on the Profiled Devices tab allows you to export the device data displayed in the tab.

1. Click **Users & Hosts > Profiled Devices**.
2. A list of devices is displayed.
3. At the bottom of the window in the **Export to:** section select the file format for the export file.
4. Either save or open the file created.

Implementation

The initial implementation of device profiler is performed by a FortiNAC administrator. Day-to-day management of device profiler can be done by an administrator with an administrator profile, referred to here as a Device manager profile. This section of the documentation outlines the implementation process in the order in which it should be done.

Administrator

Administrators have full rights to all parts of the FortiNAC system and can fully implement device profiler without needing a Device manager user to manage devices. However, in most organizations these responsibilities are divided up. To begin implementing device profiler, you must do the following:

- Create or modify device profile rules that help identify new devices. See [Device profiling rules on page 259](#).
- If you plan to have a Device manager manage new devices you must create a Device manager administrator profile that can be attached to an administrator and provide the appropriate permissions. Keep in mind that an administrator profile can be created so that the same administrator can also be responsible for guest manager. Guest manager permissions are provided via an administrator profile. See [Profiles for device managers on page 256](#).
- Once the Device manager administrator profile has been created with the appropriate permissions, you must attach that profile to an administrator. Administrators can only have one profile attached. See [Add an administrator on page 257](#).
- If you decide to use the role-based access features of FortiNAC for hosts managed in Inventory you must go to role management and configure settings for the device roles. You can create and use additional roles also. In this case, the devices that are managed by device profiler are considered hosts. Roles are assigned to devices as they are added to FortiNAC. Every device and host must have a role. If no role is selected, devices and hosts are added to the NAC Default role. See [Roles on page 620](#) for additional information.
- For hosts managed in the Hosts View role is an attribute of the host and can be used as a filter in user/host profiles. Those profiles determine which network access policy, endpoint compliance policy, Supplicant EasyConnect Policy and Portal Policy is applied. See [Policy & Objects on page 457](#).
- Device profiler processes can generate events and alarms that you may want to monitor. See [Events and alarms on page 259](#).
- Device Profiling rules allow you to limit access to the network based on time of day or day of week. During the time that the device is not allowed to access the network it is marked "At Risk" for the Guest No Access admin scan. If you choose to implement this feature for any rule, the following requirements must be met:
 - You must have a quarantine or remediation VLAN on your network.
 - Ports through which a device would connect must be in the Forced Remediation Group (applies only to wired ports). See [Groups on page 843](#).
 - Access time can only be enabled for rules that register a device in the Host View.
 - The Model Configuration for all switches to which devices connect must have an entry for the quarantine VLAN. This applies to both wired and wireless switches and access points. See [Model configuration on page 338](#).
 - Access time can only be enabled for rules that register a device in the Host View or both Host View and Inventory.

Device manager

Device managers have the following responsibilities. Administrators can perform these functions also.

Device managers can manage devices or end-stations that have been categorized by device profiler. Management options include registering, deleting and enabling/disabling devices. In addition, the Device manager can add notes to a device record and export a list of records in multiple formats. See [Configure profiled devices on page 252](#) for more information.

Profiles for device managers

In FortiNAC, you can create an administrator and give that user an administrator profile that contains permissions for the device profiler feature set. These privileges are designed to restrict this user to certain parts of the program.

For device profiler, the administrator profile, referred to as a Device manager in documentation, requires permission for Profiled Devices. This allows the user to manage new devices and categorize them.

Additional permissions can be given to Device Managers based on the parameters of their responsibilities. Create one or more administrator profiles for these types of users. See [Administrator profiles on page 125](#).

Device profiler

This procedure describes how to create an administrator profile for an administrator with permissions for device profiler. This user can access the **Profiled Devices** tab and use that window to register, delete, enable or disable hosts and enter notes about a host. The **Profiled Devices** window displays devices that are treated as hosts and are also displayed in the Host View.

You can have an administrator profile that allows an administrator to perform additional tasks by adding more permission sets. These step-by-step instructions assume that the administrator profile will provide permissions only for device profiler. Details on other settings and permissions sets see [Add an administrator profile on page 139](#).

1. Click **Users & Hosts > Administrators > Profiles**.
2. Click **Add**. The **Add Admin Profile** screen appears with the **General** tab highlighted.
3. On the **General** tab, enter a name for the profile, such as Device Manager.
4. Under **Manage Hosts and Ports**, select **All**.
5. Leave the defaults for the remaining fields and click on the **Permissions** tab.
6. On the Permissions tab note that some permissions are dependent on each other. Refer to the [Permissions list on page 133](#) for additional information.
7. The minimum that this Device Manager must have is the **Profiled Devices** permission set. Select all of the check boxes for this set including the **Custom** check box.
8. When you select the Profiled Devices permission set, the Landing Page field defaults to Profiled Devices.
9. The Profile Devices tab is enabled when Custom is selected for the Profiled Devices permission set. Click on the **Profiled Devices** tab.
10. Use the table below to configure the Profile Devices specific fields.
11. Click **OK** to save.

Settings

Field	Definition
Register, Delete, and Disable Profiled Devices	If enabled, the user can register, delete and disable devices that have been profiled by device profiler.
Modify Device Rule Confirmation Settings	If enabled, the user can change rule confirmation settings on devices that have been profiled by device profiler. Rule confirmation settings control whether or not device profiler checks a previously profiled device to determine if it still meets the criteria of the rule that categorized the device.
Manage Profiled Devices Using These Rules	• All Rules: includes current rules and any rules created in the future. • Specify Rules: you must choose the rules from the Available Rules field and manually move them to the Specify Rules field.
Available Rules	Shows the existing rules you can select for this profile. Select the rule and click the right arrow to move it to the Selected Rules pane.
Selected Rules	Shows the rules you selected from the Available Rules section. The user can only access the devices associated with the rules in this list.
Add Icon	Create a new Device Profiling Rule. For information on rules, see Adding a rule on page 264 .
Modify Icon	Modify the selected Device Profiling Rule. For information on rules, see Adding a rule on page 264 .

Add an administrator

If you are creating administrators to manage guests or devices, you must create an administrator who has the appropriate administrator profile associated. See [Administrator profiles on page 125](#).

1. Select **Users & Hosts > Administrators**.
2. Select **Add**.
3. Enter an alphanumeric **User ID** for the new administrator and click **OK**.

As you enter the user ID, the network user database is checked to see if there is a current user with the same ID and a drop-down list of matching users is displayed.

If you enter an ID that already exists as a regular network user, the network user and the administrator become the same person with a single account. This allows you to give a network user administrator privileges to help with some administrative tasks.

4. Use the table of below for settings:

Field	Definition
Authentication Type	Authentication method used for this administrator. Types include: • Local: Validates the user to a database on the local FortiNAC appliance. • LDAP: Validates the user to a directory database. FortiNAC uses the LDAP protocol to communicate to an organization's directory. • RADIUS: Validates the user to a RADIUS server.

Field	Definition
Admin Profile	Profiles control permissions for administrators. See Administrator profiles on page 125. • Add: Opens the administrator profiles window allowing you to create a new profile without exiting the Add User window. • Modify: Allows you to modify the selected administrator profile. Note that modifications to the profile affect all administrators that have been assigned that profile.
User ID	Unique alphanumeric ID for this user.
Password	Password used for local authentication. If you authenticate users through LDAP or RADIUS, the password field is disabled and the user must log in with his LDAP or RADIUS password.
First Name	User's first name.
Last Name	User's last name.
Address	Optional demographic information.
City	
State	
Zip/Postal Code	
Phone	
E-mail	E-mail address used to send system notifications associated with features such as alarms or profiled devices. Also used to send guest self registration requests from guests requesting an account. For multiple e-mail addresses, enter addresses separated by commas or semi-colons. Messages are sent to all e-mail addresses provided.
Title	User's title, such as Mr. or Ms.
Mobile Number	Mobile Phone number used for sending SMS messages to administrators.
Mobile Provider	Mobile provider for the mobile phone number entered in the previous field. Used to send SMS messages to administrators. This field also displays the format of the SMS address that will be used to send the message. For example, if the provider is US Cellular, the format is xxxxxxxxx@email.uscc.net, where the x's represent the user's mobile phone number. The number is followed by the email domain of the provider's message server.
Notes	Free form notes field for additional information.
User Never Expires	If enabled, administrators are never aged out of the database. The default is enabled.  Administrators assigned the System Administrator profile cannot be aged out.

Field	Definition
Propagate Hosts	The Propagate Hosts setting controls whether or not the record for the host owned by the user is copied to all managed FortiNAC appliances. This field is only displayed if the FortiNAC server is managed by a FortiNAC Control Manager.

- Click **OK** to save the new user.

Events and alarms

Certain actions within device profiler generate events that appear in the Event Log. Examples of device profiler events are listed in the following table.

Event	Definition
Device Profile	Generated whenever device profiling updates a rogue.
Device Profile Rule Match	A rogue host has matched a Device Profiling rule allowing it to be assigned a device type and registered.
Device Profiling Automatic Registration	A rogue host has been registered by device profiling based on a device profiling rule.
Device Profiling Rule Missing Data	Indicates that device profiler cannot compare a rogue against a rule because FortiNAC does not have enough information about the rogue, such as a DHCP fingerprint. If device profiler cannot compare a rogue against a rule it does not continue processing that rogue, and moves on to the next rogue.
Device Rule Confirmation Success	Devices identified by a Device Profiling rule maintain their association with that rule. If enabled, the associated rule and the device are checked periodically to see if the rule is still valid for the device. These event messages indicate whether or not the device matched the associated rule.
Device Rule Confirmation Failure	

Events can be mapped to alarms. Alarms can be set to notify an administrator when they are triggered. Alarms can also be viewed on the Alarms Panel on the dashboard. For more information on events and alarms, e-mail notifications, and how to map events to alarms see [Map events to alarms on page 784](#).

Device profiling rules

Device profiling rules are used by the device profiler feature to categorize rogue hosts that connect to the network. As a rogue connects to the network and receives an IP address its information is compared to all methods within each enabled rule in turn until a match is found. The rogue device can be managed in a variety of ways depending on the configuration of the rule.

Any of the following scenarios could result from a match.

- The rogue matches a rule and is placed in the Inventory as a device. It cannot be seen in the Profiled Devices window and cannot be managed by a Device manager. Future rules cannot be run against this device unless it is deleted from the system and becomes a rogue again when it connects to the network.

- The rogue matches a rule and is registered. It is displayed in the Host View as a registered host and can be seen in the Profiled Devices window. It remains associated with the matching rule and can be managed by a Device manager. Future rules cannot be run against this device unless it is deleted from the system and becomes a rogue again when it connects to the network.
 - The rogue matches a rule and is registered. It is displayed in the Host View as a registered host and is associated with a specific user, thus creating an identity for that device. It is removed from the Profiled Devices window and cannot be managed by a Device manager. Future rules cannot be run against this device unless it is deleted from the system and becomes a rogue again when it connects to the network.
 - The rogue matches a rule, but the rule is not configured to place the device in Inventory or Host View. The device remains a rogue, but is associated with the rule. Future rules can be run against this device as long as it remains unregistered. The device can be seen in the Profiled Devices window. If **Notify Sponsor** is enabled, the Device manager receives an e-mail that there was a match. The device can be managed by the Device manager. The Device manager can register the device which places it in the Host View or can delete the device. An administrator can access the device in the Host View and change it to a device if it needs to be in Inventory.
- Device profiler does not see devices that are no longer rogues and cannot match those devices with new or modified rules.

In summary, Devices placed in the Inventory only cannot be seen in the Profiled Devices window. Devices placed in the Host View display in the Profiled Devices window until the device is associated with a user. Devices placed in both Host and Inventory display in the Profiled Devices window until the device is associated with a user.

Host view vs. Inventory

Device profiling rules can be used to place rogue devices in the Hosts, in Network > Inventory or both. There are certain advantages to each option that should be kept in mind when determining where to place a device.

Devices that are kept in the Host View have a connection history and can be associated with a user. Devices that are placed in the Inventory can be polled for their connection status. Devices that are not connected display in red on the Inventory. If the connection to the device fails, events and alarms can be configured to notify you that the device is no longer communicating.

Managing rules

The Device Profiling Rules view displays the default set of rules provided. Use this window to modify the default rules or to create your own set of rules. Default rules vary depending on the version of the software and the firmware installed. Upgrading to a newer version of the software does not add or modify default rules.

Disabled rules are ignored when processing rogues. Device Profiling rules are disabled by default and are set not to register devices. When you are ready to begin profiling, enable the rule or rules you wish to use.

Enabling certain rules could result in all unregistered devices on your network being displayed in the Profiled Devices window. Review each rule carefully before enabling it.

The **Catch All** rule is always at the end of the list and its rank cannot be changed. As new rules are added they are inserted into the list immediately above the Catch All rule. This guarantees that all rogues profiled by device profiler are associated with a rule and can be managed by an administrator with the appropriate administrator profile, a Device manager. Device managers cannot manage devices that are not associated with a rule. This rule has no identification methods and no device type.

Device profiling rules created on the FortiNAC will be ranked above global device profiling rules created on the FortiNAC Manager. The rank of a local Device Profiling Rule can be adjusted above or below another local Device Profiling Rule,

but cannot be ranked below a global Device Profiling Rule. The rank for a global Device Profiling Rule cannot be modified from the FortiNAC.

Settings

An empty field in a column indicates that the option has not been set.

Field	Definition
Add	Add a device profiling rule. See Adding a Rule .
Modify	See Adding a Rule .
Delete	See Deleting a Rule .
Copy	See Copying a Rule .
Run	Used to re-run the device profiler process when rules have been modified or added. Devices that have already been categorized are not affected. Only rogues that remain in the Host View are processed. If rules are set to notify Device managers via e-mail when rogues connect, processing existing rogues triggers those e-mails again. Rogues that are no longer connected are ignored.
Import	Imports data from a selected XML file. File must be of type XML.
Export to	Exports the displayed data to a file of the selected type in the default downloads section. File types include CSV, Excel, PDF, RTF, and XML.
Rank	Moves the selected rule up or down in the list. Devices are compared to rules in order by rank.
Set Rank Button	Allows you to type a different rank number for a rule and immediately move the rule to that position. In an environment with a large number of rules this process is faster than using the up and down Rank buttons. Rank can only be set on local policies, rank changes for global policies must be done at the FortiNAC Manager.
Enable/Disable	Enables or disables the selected rule. If a rule is disabled it is not used when processing a rogue host.
Rogue Evaluation Queue Size	Indicates the number of Rogues waiting to be processed by the device profiling rules. The queue is filled by Rogues as they connect to the network. If you select Run , any rogues that were not previously categorized are added to the queue immediately. This number moves up and down as the system processes rogues. Detail: Rogue Evaluation and Rule Confirmation queue performance information: - Number of scans requiring an IP address - Number of scans with an IP address - Average time in the queue - List of rules with the number of pending scans for each rule Flush: Deletes any hosts remaining in the Rogue Evaluation queue. Note: Does not clear the Rule Confirmation queue.

Field	Definition
Name	User defined name for the rule.
Type	Device type that is assigned when the rule is a match for a rogue host.
Registration	Indicates whether devices matching this rule are registered automatically or manually.
Methods	The method or methods used to identify a device. Methods include: IP Range, DHCP Fingerprinting, Location, TCP, NMAP, Passive Fingerprinting, RADIUS Request, Vendor OUI and UDP.
Register as Device	When a device is registered it can be placed in the Host View, the Inventory, or both. This column indicates where the device is placed when it is registered. If the column is blank, then the registration option has not been set for this rule.
Notify	A green check mark indicates that Notify is enabled. When a new device is detected and it matches this rule, an email is sent to all Device managers that have this rule associated with their administrator profile. A red circle indicates that the Notify option is disabled.
Role	Role assigned to devices matching this rule.
Access Availability	Times that devices matching this rule are permitted to access the network. Devices matching this rule are marked "At Risk" for the Guest No Access admin scan during the times they are not permitted to access the network.
Add to Group	Devices matching this rule are added to the group displayed. Add to Group is only available for devices that are added to the Host View.
Container	Devices matching this rule are added to the Container displayed. Devices can only be placed in a Container if they are being added to the Inventory.
Confirm Rule On Connect	If enabled, device profiler confirms that previously profiled devices associated with this rule still match this rule the next time they connect to the network. A green check mark indicates that the option is enabled. A red circle indicates that the option is disabled.
Confirm Rule Interval	If enabled, device profiler confirms at set intervals that previously profiled devices associated with this rule still match this rule.
Confirmation Failure Action	If enabled, device profiler disables previously profiled devices that no longer match their associated rule.
Last Modified By	User name of the last user to modify the rule.
Last Modified Date	Date and time of the last modification to this rule.
Right click options	
Copy	Copy the selected Rule to create a new record.
Delete	Deletes the selected Rule(s). Removes the association between that rule and the devices it matched. Devices associated with deleted rules will no longer display in the Profiled Devices window.

Field	Definition
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746  You must have permission to view the admin auditing log. See Add an administrator profile on page 139.
Modify	Opens the Modify Device Profiling Rule window for the selected rule.

Best practices

The configuration of Device Profiling rules should be considered carefully to optimize performance. The list below outlines concepts that should be taken into account when configuring rules.

1. When a device or host connects to the network, the device profiling rules are checked in order starting with the rule ranked number 1. The order of the rules is important. For the best performance, it is recommended that you rank rules based on the Methods used to categorize devices and hosts as follows: OUI rules first, DHCP rules next and Active, TCP/UDP port, IP Range, Location rules last.
In an environment where static IP addresses are used, DHCP rules should be at the end of the list. Devices with static IP addresses do not send out DHCP broadcast packets. Therefore, FortiNAC will never receive a DHCP fingerprint for those devices and the profiling process will not continue past the DHCP rules.
It is recommended that you set up IP Helper addresses for DHCP on your routers when using DHCP fingerprinting. Use the IP address of port1 on the FortiNAC Server.
2. The device information necessary to compare against a rule, must be available for device profiler to successfully move from one rule to the next. If the information required for a rule to be matched is unavailable, the evaluation of that device ends. For example, if the IP address of the device cannot be determined, device profiler cannot move past any rule that uses IP address as match criteria. The reason that the device profiler does not skip the rule and continue with the next one is that combinations of rules would not work. In the example below, if the device profiler skips the first rule because the TCP port cannot be found, the Apple iPhone will be miscategorized. If the device profiler does not skip the rule, Apple iPhone remains uncategorized and the user can either manually determine what the device is or can adjust the rules to catch it.

Example:

This example outlines how two rules can be used together to provide greater accuracy when profiling devices. Apple iPhone and MAC OS fingerprints tend to be almost identical, but the iPhone can be distinguished by a TCP port which can be used in a rule to identify that device. In this case, you can create two rules: the first to identify iPhones by scanning for the iPhone TCP port and the second to scan for MAC OS in general. The iPhone rule is more granular and will catch the phone before it is categorized by the MAC OS rule.

3. OUI only rules are the quickest to process because no outside data is necessary.
4. Rules that require an IP address take longer to process because the FortiNAC server may need to read the DHCP leases file or layer 3 tables from the routers.
5. Device profiler uses the latest IP address from the IP-to-MAC cache, if the IP address exists. It does not rely on the IP address seen in the **Adapter View** because it may be stale. If the IP address does not exist in the cache, FortiNAC starts an IP –to-MAC lookup on all L3 devices. FortiNAC stops the lookup as soon as the address is found, therefore, in most cases every L3 device will not be polled. If the FortiNAC server is not properly configured to read layer 3 from the routers, it may cause Device Profiling rules that require an IP address to fail.

Adding a rule

1. Go to **Users & Hosts > Device Profiling Rules**.
2. Click **Add**.
3. In the **General** tab, select **Enabled**.
4. Enter a **Name**, **Description**, and **Note**.
5. (Optional) Select **Notify Sponsor**. If selected, administrators with permission to manage devices associated with this rule are notified when a new device matches the rule.
6. Use the table below to configure **Registration Settings**:

Registration	Automatic: The device is registered immediately if the Register as option is selected. Manual: The device is registered manually from Profiled Devices. Register as must be selected in order to manually register the device.
Type	Select the device category in which a device matching this rule is placed. To create a new type, click . In version F 7.6.3, this list has been expanded to reflect the updated device type database integrated with FortiGuard. Admins can now select from a significantly broader set of device types, enabling more precise classification and profiling based on the enhanced FortiGuard Category/Subcategory mappings.
Role	If you are using role-based access for hosts and devices managed in Inventory, select the role that controls access to the network for this device. If you are not using role-based access, select NAC-Default. To create a new role, click .
Register as	Select where the registered device is placed. Options include: • Device in Host View • Device in Topology (if you select this option, select the Container) • Device in Host View and Topology (if you select this option, select the Container) • Host to User (if you select this option, enter the User ID) • Host to Logged In User (If Present) If the device is an access point and you register it in Host View, it is removed from Host View and moved to Inventory after the first poll. It is also removed from the concurrent license count once it is recognized as an access point.
Add to Group	Select this option to add the device to a group. This option is not available if Register as is set to Device in Topology. To create a new group, click .
Access Availability	Determine when devices that match this rule are permitted to access the network. You can either select Always or specify a time.

7. Select the appropriate **Rule Confirmation Settings**:

- **Confirm Device Rule On Connect**: Check that a previously profiled device still matches the rule every time it connects.
- **Confirm Device Rule On Interval**: Check that a previously profiled device still matches the rule at regular time intervals. You can set the interval for a set number of minutes, hours, or days.
- **Disable Device If Rule No Longer Matches Device**: Disable a previously profiled device if it no longer matches the rule.

8. In the **Methods** tab, select one or more methods to use for device identification. The device must meet the criteria established for all of the methods selected to match the rule.

Use the table below to select the method(s):

Active	Select a method to determine rule matching using information collected Network sessions. For additional details, see Network sessions in the Administration Guide: • Match Type: Matches if the device type selected corresponds to the Operating System of the device being profiled. • Match Custom Attributes: Matches if the manually entered host name and/or Operating System corresponds to the device being profiled. Enter either an exact string match or regular expression to match. You must configure firewall session polling to use this method. For more information, see Firewall session polling.
DHCP Fingerprinting	It is recommended to set up IP helper addresses for DHCP on routers when using DHCP fingerprinting. When evaluating a host using the DHCP fingerprint method, FortiNAC compares the last DHCP packet received. Previous entries evaluated are considered historical. Select a method to determine rule matching with DHCP: • Match Type • Match Custom Attributes ◦ Fields left blank are ignored. ◦ For best performance, it is recommended to make custom strings only as specific as necessary to match appropriately: i. Define a parameter list. Avoid wildcarding the parameter list (example: 1,3,252,42,*). ii. If criteria is not specific enough to match properly, add hostname or vendor class second. iii. If criteria is not specific enough to match properly with parameter list and hostname or vendor class, add "Option List" or "Message Type".
HTTP/HTTPS	Determine rule matching by sending an HTTP/HTTPS request. Select the Protocol, Port, and Path used to send requests to the device. If required, select Authentication and enter user credentials. (Optional) Select Match and enter a response message. If you enter multiple response values, the device matches if any of the values are found.
IP Range	Click Add and enter an IP range to match. Examples:

	Starting IP: 10.10.124.140 Ending IP: 10.10.124.180 Wildcard examples: Starting IP: 10.10.124.* Ending IP: 10.10.125.* Starting IP: 10.10.*.140 Ending IP: 10.10.*.180 Starting IP: *.*.*.140 Ending IP: *.*.*.180
Location	Click Add and select the container(s) to match.
Passive	Select a Match Type to use with passive fingerprinting.
Persistent Agent	Set Match Type to an operating system. To use this method, devices must have a FortiNAC agent installed. To register hosts running the Persistent Agent using this method, you must disable registration under Persistent Agent Properties. For more information, see Credential configuration on page 918.
RADIUS Requests	Local RADIUS Access Requests will add endpoint fingerprints which can be used in Device Profiling rules to profile devices post-connect.
SNMP	Determine rule matching by sending an SNMP GET request for the OID specified. • OID: Enter OID to be queried (required) Example: 1.3.6.1.2.1.1.1.0 • Port: Enter the port used for SNMP (required - Default is 161) • Under SNMP V1/V2c and/or SNMP V3 (required): Click Add and enter security credentials. If multiple credentials are entered, the device matches if any of the credentials are found. (Optional) Select Match and enter a response string. If you enter multiple string values, the device matches if any of the values are found.
SSH	Determine rule matching by sending an SSH client session request. Credentials: Click Add and enter user credentials. If you enter multiple credentials, the device matches if any of the credentials are found. Commands: Click Add and enter commands for the request. The possible commands are: • expect: A regular expression string that matches the response from the device. • send: A string sent to the device that has two keywords, %USERNAME% and %PASSWORD%. A series of commands can be configured as an automated way to interact with the CLI on the device. The commands are executed in order, starting from the top. Only a single command can be executed at a time. Multiple commands cannot be chained together (pipes " " are not supported).

Example

expect: User Name:
send: %USERNAME%\n
expect: Password:
send: %PASSWORD%\n
expect: Dell-3324#
send: show system\n

(Optional) Select **Match** and enter a response string. If you enter multiple string values, the device matches if any of the values are found.

TCP

Click **Add** and enter a TCP port to match. You can enter multiple ports, separated by commas, or a port range using a hyphen. If you enter multiple ports, all ports must match.

Telnet

Determine rule matching by sending a telnet client session request.

(Optional) Click **Add** and enter user credentials. If you enter multiple credentials, the device matches if any of the credentials are found.

Click **Add** and enter commands for the request. The possible commands are:

- **expect:** A regular expression string that matches the response from the device.
- **send:** A string sent to the device that has two keywords, %USERNAME% and %PASSWORD%.

(Optional) Select **Match** and enter a response string. If you enter multiple string values, the device matches if any of the values are found.

UDP

Click **Add** and enter a UDP port to match. You can enter multiple ports, separated by commas, or a port range using a hyphen. If you enter multiple ports, all ports must match.

Vendor OUI

Determine rule matching using the vendor OUI.

Click Add to configure an OUI. You can add the following field types:

- **Vendor Code:** To use a vendor code, enter the first characters in the code, then select a code from the available list.
- **Vendor Name:** To use a vendor name, enter the first characters in the name, then select a code from the available list. You can use a wildcard (*) at the beginning and end of the vendor name.
- **Vendor Alias:** Enter a vendor alias that exists in the FortiNAC vendor database. You can use a wildcard (*) at the beginning and end of the vendor alias.
- **Device Type:** Select a device type. If you select this option, the device type associated with the connecting device must match the device type for the vendor in the FortiNAC database.

For more information, see [Vendor OUIs on page 898](#).

Note: Invalid Physical Addresses: If the MAC address matches a rule, the host will be registered regardless if vendor OUI is in the database. Device Profiler does not check to determine if the MAC address is valid.

WinRM

Determine rule matching by sending a WinRM client session request.

Click **Add** and enter user credentials. If you enter multiple credentials, the device matches if any of the credentials are found.

	Click Add and enter commands for the request. (Optional) Select Match and enter a response string. If you enter multiple string values, the device matches if any of the values are found. For more information on requirements and setup, see WinRM Device Profile Requirements and Setup on page 270.
WMI Profile	Determine rule matching by sending a WinRM or SSH client session request and creating a WMI profile. Set Protocol to WinRM or SSH and enter the Port. Click Add and enter user credentials. If you enter multiple credentials, the device matches if any of the credentials are found. Additional options allow you to match specific versions of Microsoft Windows, installed applications, Windows Service statuses, running processes, serial numbers, and asset tags (with wildcard matching). For more information on requirements and setup, see WinRM Device Profile Requirements and Setup on page 270.
Network Traffic	Determine rule matching using network flow. Set Protocol to TCP, UDP, or Other. Enter the Destination Port. (Optional) Enable Apply Destination as Source Device and enter the Destination IP. One or both of the following must be configured to use this method: • Firewall session polling. For more information, see Firewall session polling. • FortiNAC-OS requirement: "set allowaccess" command option "netflow". See Open Ports for details.
FortiGate	Select a method to determine rule matching using information collected Network sessions. For additional details, see Network sessions in the Administration Guide: Match Type: Matches if the device type selected corresponds to the Operating System of the device being profiled. Match Custom Attributes: Matches if the manually entered host name and/or Operating System corresponds to the device being profiled. Enter either an exact string match or regular expression to match. You must configure firewall session polling to use this method. For more information, see Firewall session polling.
ONVIF	Determine rule matching using ONVIF. • Select Add to define the ONVIF profiles that the device must support. ◦ Profile A – For products used in an electronic access control system ◦ Profile C - For door control and event management systems. ◦ Profile G - For IP-based video systems. A Profile G device (e.g., an IP network camera or video encoder). ◦ Profile Q - For IP-based video systems and its aim is to provide quick discovery and basic configuration of Profile Q conformant products (e.g., network camera, network switch, network monitor) on a network.

	◦ Profile S - For IP-based video systems. A Profile S device (e.g., an IP network camera or video encoder) ◦ Profile T - For IP-based video systems. Profile T supports video streaming features such as the use of H.264 and H.265 encoding formats. • (Optional) Select Match and enter a response string. If you enter multiple string values, the device matches if any of the values are found.
FortiGuard	This method pulls IoT device information from the FortiGuard IoT Service based on the MAC address. Note: • Requires FortiCare support contract to enable FortiGuard IoT Service. Otherwise, the checkbox will not be selectable. • IoT service responses are enhanced when the "FortiGuard Collect Service" is enabled in Users & Hosts > Settings > Device Profiler Match Type • The Fortinet IoT query service is used to determine the OS of the device. Matches if the device type selected corresponds to the Operating System of the device being profiled. Match Custom Attributes • Category • Subcategory • Vendor • Model • Operating System • Sub Operating System
Script	Execute one of the command line scripts located in <code>/home/cm/scripts</code>. These command line scripts are for advanced use, such as administrator-created Perl scripts. MAC address and IP Address are passed to the script as arguments. Matches if the exit status of the script is zero.

9. Click **OK**.

Deleting a rule

When a Device Profiling Rule is deleted the association between that rule and the devices it matched is removed. Devices associated with that rule will no longer display on the Profiled Devices window. They will continue to display in the Host View.

The **Catch All** rule is a default system rule that cannot be removed. Other default rules can be removed.

1. Click **Users & Hosts > Device Profiling Rules**.
2. Click select a rule and click **Delete**.
3. A message displays asking if you are sure. Click **Yes** to continue.

Copying a rule

1. Click **Users & Hosts > Device Profiling Rules**.
2. Click select a rule and click **Copy**.
3. The Add Device Profiling Rule window displays with the information from the selected rule.
4. You must, at minimum, modify the name of the rule. Modify other fields as needed and click **OK** to save.
5. For Settings, see [Adding a rule on page 264](#).

Evaluating rogue hosts

Over time you may have hosts that remain rogues because they do not match any of the rules enabled in the device profiling rules. You may also have hosts that have been categorized incorrectly. At any time you can modify the rules or create additional rules and then re-evaluate hosts. Only those hosts that remain unregistered can be re-evaluated.

If a host has been categorized incorrectly and has been registered, you have two options. Either manually modify the host or delete the host and when it connects to the network again, it will be evaluated by the rules.

Rogues that are no longer connected or are offline are ignored.

1. Click **Users & Hosts > Device Profiling Rules**.
2. Click **Run**.
3. A message displays asking if you would like to evaluate rogues. Click **Yes** to continue.
4. A new message displays indicating that x number of rogues are being evaluated.
5. Device profiler compares any rogue hosts to the list of enabled device profiling rules and processes them accordingly. See [How it works on page 251](#) for additional information.
6. When the process is complete, click **OK** to close the message box.

WinRM Device Profile Requirements and Setup

Requirements:

- WinRM service must be enabled on endpoints.
- The WinRM HTTP port(s) (5986 or 5985 (insecure)) must be enabled and available through the firewall to the FortiNAC App. server. HTTPS (5986) is strongly encouraged for security purposes.
- NTLM Authentication with domain credentials authorized to run powershell commands get-wmiobject, get-itemproperty, get-service, get-process, convertto-json, and read the registry.
- Minimum Windows Management Framework (WMF) version: 3.0

Supported Windows Versions:

Windows Server 2008 R2 SP1 - With WMF 3.0	Windows 10 (All versions)
Windows 7 SP1 - With WMF 3.0	Windows Server 2016
Windows 8.1	Windows Server 2019
Windows Server 2012 R2	

Endpoint Setup Instructions

If desired, the configuration of domain endpoints to support WinRM can be done through these steps. They are required to configure a secure HTTPS connection from FortiNAC to endpoints using WinRM. The following settings should be the result:

- WinRM Listener on port 5986 with transport HTTPS
- Certificate enrollment resulting in a certificate on the endpoint with hostname as subject (e.g. CN=hostname.example.com) and "Server Authentication" key usage.
- Inbound Windows Firewall rule for port 5986
- Windows Remote Management service enabled.



If you want to fore go security, you can use alternate steps to configure and use HTTP while allowing unencrypted content. However, this is not recommended for security reasons.

1. Open Windows PowerShell or a command prompt. Run the following command to determine if you already have WinRM over HTTPS configured:

```
winrm enumerate winrm/config/listener
```

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> winrm enumerate winrm/config/listener
Listener
  Address = *
  Transport = HTTP
  Port = 5985
  Hostname
  Enabled = true
  URLPrefix = wsman
  CertificateThumbprint
  ListeningOn = *
```

If you see a listener on port 5986 with Transport = HTTPS, WinRM over HTTPS is already configured and no further steps are necessary.

2. If WinRM over HTTPS is not already configured, run the following command on a typical domain-joined workstation as an administrator:

```
winrm quickconfig -transport:https -force
```

If an error is returned indicating there is no appropriate certificate, a certificate template will need to be configured for enrollment. Other wise, run step 1 again. If a listener is shown, skip to the Group Policy Configuration.

Create a Certificate Template

1. Open Active Directory Certificate Services. This can be done through the Server Manager or from Administrative Tools.
2. Expand the Certificate Authority (CA) and select **Certificate Templates**. Select **Action > Manage**.
3. Select the Workstation Authentication template. Select **Action > Duplicate**.
4. Change Template Display Name to FortiNAC WinRM

-
5. Select the **Subject Name tab > Build from this Active Directory Information**. Fill in the following fields:
 - a. **Subject name format:** DNS name
 - b. **Alternate subject name:** DNS name
 6. Select **Security tab > Application Policies > Edit > Add > Server Authentication**.
(Optionally, select **Client Authentication** and click the **remove** button)
 7. Select **OK** to dismiss the **Edit Application Policies Extension** dialog.
 8. Select **OK** to dismiss the **FortiNAC WinRM Properties** dialog.
 9. Close the window.
 10. Select **Certificate Template** and choose **Action > New > Certificate to issue**
 11. Choose **FortiNAC WinRM** and select **OK**.
 12. If required, create a new Group Policy Object for Certificate Enrollment.

Create a Group Policy Object to configure WinRM

1. Create a Group Policy Object (GPO) named `FortiNAC WinRM`
2. Select the GPO and choose **Action > Edit**
3. Navigate to **Computer Configurations > Policies > Windows Settings > Security Settings > System Services**
4. Double-click Windows Remote Management (WS-Management)
5. Tick the box for **Define this policy setting** and select **Automatic**.
6. Select **OK**
7. Navigate to **Computer Configurations > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Expand > Inbound Rules**
8. Right-click and select **New Rule**
9. Select **Port > Next > TCP**. Enter `5986` in **Specific local ports**. Select **Next**.
10. Select **Allow the Connection > Next**.
11. Un-tick the box for **Private** and **Public**. Leave only **Domain** ticked.
12. Name the rule `WinRM HTTPS for FortiNAC`. Select **Finish**.

Optionally, restrict to your FortiNAC Application Server IP Address.

1. Double-click the rule.
2. Click the scope tab
3. Under Remote IP Address, select **These IP Addresses**
4. Select **Add** and enter the addresses for your FortiNAC appliances.
5. Navigate to **Computer Configuration -> Policies -> Windows Settings -> Scripts (Startup/Shutdown)**
6. Double-click Startup
7. Select **Show Files**
8. Create a new batch file or other script you're comfortable with. Name it `winrm-enable.bat`
9. The contents of the file should be the following command:
`winrm quickconfig -transport:https -force`
10. Select **Add > Browse**
11. Select `winrm-enable.bat`
12. Select **OK** to dismiss any dialogs.
13. Close the Group Policy Management Editor
14. Link the FortiNAC WinRM GPO as needed

Alternate steps to configure WinRM.



Typically insecure configuration

1. Create a GPO `FortiNAC WinRM`
2. Select the GPO and choose **Action->Edit**
3. **Navigate to Computer configuration -> Policies -> Windows Settings -> Security Settings -> System Services**
4. Double-click **Windows Remote Management (WS-Management)**
5. Tick **Define this policy setting** and select "Automatic"
6. Click **Ok**.
7. Navigate to **Computer configuration -> Policies -> Windows Settings -> Security Settings -> Windows Firewall with Advanced Security -> Expand -> Inbound Rules**
8. Right-click and select **New Rule**
9. Select **Predefined > Windows Remote Management > Next**
10. Untick the compatibility mode which opens port 80 and click **Next**.
11. Select **Allow the Connection** and click **Finished**.

Optionally, restrict to your FortiNAC Application Server IP Address.

1. Double-click the rule.
2. Click the scope tab
3. Under Remote IP Address, select **These IP Addresses**
4. Select **Add** and enter the addresses for your FortiNAC appliances.
5. **Navigate to Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Windows Remote Management (WinRM) -> WinRM Service**
6. Enable **Allow remote server management through WinRM** with * as the IPv4 and IPv6 filters.
7. Enable **Allow unencrypted traffic**
8. Close the Group Policy Management Editor
9. Link the FortiNAC WinRM GPO as needed.

Network sessions

The **Network Sessions** page displays a list of sessions on your network. FortiNAC receives information about these sessions from the following sources:

- FortiGate devices via Firewall Session Polling (see [Firewall session polling](#))
- Netflow traffic (see [Netflow support](#))

To view sessions, go to **Users & Hosts > Network Sessions**. To export this data in CSV, Excel, PDF, or RTF format, click the appropriate icon.

Using filters

1. Use the **Add Filter** drop-down menu to select a filter type from the following options:
 - Country
 - Destination address
 - Destination MAC address
 - Destination port
 - Device
 - Firewall
 - Hostname
 - Protocol
 - Source address
 - Source MAC address
 - Source port
2. Enter a name or number for the filter.
3. Use additional filters as required. You can only have one of each type of filter.
4. Click **Update**.

Creating a device profiling rule

There are two methods to create a device profiling rule that matches any session in the list:

- Right-click the device and click **Create Device Profiling Rule**.
- Highlight the device and click **Options > Create Device Profiling Rule**.

Add Device Profiling Rule appears. Review the settings and click **OK**.

For more information, see [Profiled devices on page 251](#).

Deleting a session

There are two methods to delete a session from the list:

-
- Right-click the device and select **Delete**.
 - Highlight the device and click **Options > Delete**.

Locate hosts

Click **Users & Hosts > Locate Hosts** on the dashboard to locate devices, users or hosts by changing the Search Type.

Locate devices or hosts

1. Select **Users & Hosts > Locate Hosts**.
2. Select a search type.

Search Type	Description
All	This option searches for both devices and hosts.
Devices	Use this option to locate network devices.
Hosts/Users	Use this option to locate hosts or users.

3. Enter the search criteria. To reduce the potential for a significant number of records being returned in the search results, you must enter a value into one of the search fields.
If the search type is set to **All** and you enter data in the **Name** field, FortiNAC searches for user last names and network device names.
4. Click **Search**.

Locate hosts and users

This window can be used to search your database for hosts and users of many types. Guests, contractors and conference attendees are also considered users and can be located using this window or through the **Guest/Contractor Accounts** window. See [Guest or contractor accounts on page 1](#).

You cannot locate guest or contractor accounts until the account is automatically created on the specified date. For example, a contractor account scheduled for March 1 cannot be located until that date.

Use the **Locate** window to:

- Check that a record for a host exists.
- See where the host is on the network.
- Check the connect status and access of the host.
- Search for a registered host by MAC address to see where it is on the system.
- Use wild cards to search for hosts or users. See [Wild cards on page 35](#) for additional information.

Locate hosts

1. Select **Users & Hosts > Locate Hosts**.
2. Select **Hosts/Users** from the **Search Type** drop-down list.

3. Enter the **Search** criteria.

4. Click **Search**.

Fields

Field	Description
Registered hosts/devices	
Last Name	Last name of a user associated with the registered host or the vendor name of a rogue host.
IP address	IP address of the host.
Additional adapter info	
MAC Type	MAC Type for the host. The available options are: Invalid, Valid or Both.
Connect State	Connect State of the adapter. Options include: Both, Off line or On line.
Access	Access state of the adapter. Options include, Enabled, Disabled or Both.
Physical Address	MAC address of the adapter on the host.
Media Type	Searches the Media Type field in the Adapter Properties. Typically this would be either wired or wireless.
Access Value	Name or number of the network access identifier given to this adapter based on the state of the host and the device to which the adapter is connected, such as VLAN ID, VLAN Name or Aruba Role.
Additional host info	
Host Name	Name of the host.
Agent Version	Version number of the Persistent Agent, Mobile Agent, or Dissolvable Agent on the host.
Operating System	Operating system on the host.
Hardware	Hardware type of the host.
Host Type	Narrow the search by a specific type of host: All, IP Phone, Registered or Rogue.
Authenticated State	Include hosts on which a user has Authenticated, Not-authenticated or Both.
Security State	Include hosts that are Safe, At Risk, Pending At Risk or All. Search results for Safe hosts include Pending At Risk hosts. Pending At Risk is a subset of Safe hosts.
Persistent Agent	The Persistent Agent usage of the host. Options include: • No Agent: Hosts with no agent. • Agent: Hosts using the Persistent Agent. • Both: Includes both hosts that have the Persistent Agent or no Agent.
Connect State	The connect state of the adapter. Options include both, offline, or online.
Access	The access state of the host. Options include enabled, disabled, or both.

Field	Description
Host Role	Name of the Role assigned to the host. Roles are used to group hosts and are used as filters in user/host profiles.
Security & Access Value	Directory attribute used as a filter when determining which policies apply to hosts. Data contained in this field is copied from the user's account in the directory to the Security and Access value field on the User, Host and Adapter Properties. It can also be entered manually.
Additional user info	
First Name	First name of the user associated with the host.
User ID	Unique alphanumeric ID. Typically comes from the directory but if you are not using a directory, this field can be created manually.
Title	User's title, this could be a form of address or their title within the organization.
Admin Profile	Searches both administrators and network users. Options include: Any or a list of your administrator profiles. To search network users and guests or contractors, select Any.
Sponsor	If the administrator performing the search has sponsor privileges, his User Name may be filled in this field. Depending on permissions, a sponsor's search may be limited to the hosts he created and then registered. Sponsors with the ability to view all accounts can use this field to find hosts created and then registered by a specific sponsor by entering that sponsor's user name in this field.
User Role	Name of the Role assigned to the user. Roles are used to group users and as filters in user/host profiles.
Access	The Access state of the user. Options include, Enabled, Disabled or Both.
Security & Access Value	Directory attribute used as a filter in user/host profiles when determining which Policies apply to hosts. Data contained in this field is copied from the user's account in the directory to the Security and Access value field on the User, Host and Adapter Properties. It can also be entered manually.

Search results

Search results displays the host and user information and provides access to other host-specific information such as Adapter Properties, Host Properties, group membership, port properties, and Device Properties. Administrators can delete hosts, adapters and users from this view.

Column	Description
Server	Server managing the host.
Name	Last name of the user (from the user record), hostname or vendor name. This column could contain any combination of this data.
ID	ID of the host or user.
IP address	IP address of the host.

Column	Description
Physical Address	MAC address of the host.
Location	Device the host is connected to, such as a switch or a router.
Views	Icons that provide access to other related information. Click an icon to go to that view from the results window. Options include: Adapter Properties, Host Properties, group membership, Ports Properties and Device Properties.
Remove Buttons	Click the one or more check boxes in the left column to select items for deletion. Selected are removed items from the server where they were being managed. Only administrators can delete. Remove options are as follows: • Remove Host And Adapters: Deletes the selected host and all corresponding adapters. If a host has a wired and a wireless adapter, both are removed from the database. • Remove Adapter: Deletes only the selected adapter but leaves the host record, other adapter records and the user record in the database. • Remove Host Adapters And User: Deletes everything associated with the selected host from the database. • Remove User: Deletes the user associated with the selected host from the database.

Edit hosts

After searching for hosts using the Locate view, you are presented with a list of results. From within that list you can delete hosts, users and adapters, edit group membership and view adapter properties.

Delete hosts

1. Select **Users & Hosts > Locate Hosts**.
2. Enter the search criteria in the Locate view.
3. In the search results, select the check box next to the record(s) to be deleted.
4. Click **Remove** at the bottom of the window.

View or modify group membership

1. Select **Users & Hosts > Locate Hosts**.
2. Enter the search criteria in the Locate view.
3. Go to the **Views** column in the search results and click the **Group Membership** icon.
4. The groups that contain this host or user are displayed.
5. Add or remove groups as needed and click **Apply** to save changes.

If an item is placed in a subgroup, it can only be removed when viewing the membership of that subgroup. It cannot be removed from the parent group containing the subgroup.

For example, the L2 network devices group contains the Wired Devices and Wireless Devices subgroups. The Wired

Devices subgroup contains four 3COM switches. The Wireless Devices subgroup contains two Cisco switches. The L2 network devices group membership list shows all six switches, but to remove one of the 3COM switches you must go to the Wired Devices membership list.

View properties

1. Select **Users & Hosts > Locate Hosts**.
2. Enter the search criteria in the Locate view.
3. Go to the **Views** column in the search results and click the **Properties** icon.
4. The properties for the selected adapter, host or user are displayed.

Locate devices

1. Select **Users & Hosts > Locate Hosts**.
2. Select **Devices** from the **Search Type** drop-down list.
3. Enter the Search criteria.
4. Click **Search**.

Fields

Field	Definition
Name	Name of the device.
IP address	IP address of the device.
Status	The status of the device: Any : Show device regardless of current status. Management Lost : System is still in contact with the server, but the server is not managing anything. Lost : Cannot ping a known device. Unknown : Very brief status that only occurs while pinging a new device. Once the device responds to the ping the status changes. Established : Device can be pinged and is in contact.
Protocol	Protocol used to communicate with the device. Options include: Pingable, SNMP or Both.
Physical Address	Physical address of the device. If you enter a value for this option in the All or Device search, all of the device ports with a matching MAC address are shown in the results. If you do not enter a MAC address, only the device model is shown in the results.

Results

Field	Definition
Server	Name of the FortiNAC Control Server where the device is located.
Name	Name of the device.
IP address	IP address of the device.
Physical Address	MAC address of the device.
Type	Device type (vendor name/model).
Status	Contact status of the device.
Views	Icons that provide access to device specific views. Click an icon to go to that view from the results window. Options include: Device Properties, device group membership and Ports and Hosts.

Edit devices

After searching for devices using the Locate View, you are presented with a list of results. From within that list you can edit device group membership, view device properties and view the port and hosts associated with the selected device.

View/modify device group membership

1. Select Users & Hosts > Locate Hosts.
2. Enter the search criteria in the Locate Devices view.
3. Go to the **Views** column in the search results and click the **Group Membership** icon.
4. The group properties for the selected device are displayed.
5. Add or remove groups as needed and click **Apply** to save changes.

If an item is placed in a subgroup, it can only be removed when viewing the membership of that subgroup. It cannot be removed from the parent group containing the subgroup.

For example, the L2 network devices group contains the Wired Devices and Wireless Devices subgroups. The Wired Devices subgroup contains four 3COM switches. The Wireless Devices subgroup contains two Cisco switches. The L2 network devices group membership list shows all six switches, but to remove one of the 3COM switches you must go to the Wired Devices membership list.

View device properties

1. Select **Users & Hosts > Locate Hosts**.
2. Enter the search criteria in the Locate Devices view.
3. Go to the **Views** column in the search results and click the **Device Properties** icon.
4. The properties for the selected device are displayed.

View device ports and hosts

The Device Ports and Hosts results contain VLAN (Current and Default) and Host (Name and IP) information for each port on the device.

1. Select **Users & Hosts > Locate Hosts**.
2. Enter the search criteria in the Locate Devices view.
3. Go to the **Views** column in the search results and click the **Ports and Hosts** icon.
4. The ports and hosts for the selected device are displayed.

View SSIDs

All SSIDs on the device are listed with the current and default VLAN setting. If a host is connected on a port, the adapter MAC address and IP information are also displayed.

Manage hosts and ports

Manage hosts & ports contains a list of host and port groups. This view works in conjunction with administrator groups to limit administrator access. When you add an administrator to an administrator group, only the groups that the administrator has permission to manage are listed in the manage hosts & ports tab. Select a group from the list and click **Apply** to view or manage the members of the group. Click **Add Hosts** to add hosts to the database.

Add hosts

Administrators who do not have full access to the admin UI can add hosts in the Manage Hosts And Ports View. The administrator's administrator profile must have permission for Manage Hosts & Ports with Access and Add/Modify enabled.

Access add hosts

1. Select **Users & Hosts > Manage Hosts and Ports**.
2. Click **Add Hosts** at the bottom of the window.

Hosts added through this process are either registered to a user or registered as a device.

Host registered to a user

A host registered to a user is associated with that user and inherits network access parameters from the user. The host contributes to the Allowed Hosts count for the user. If the host is registered here, the user will not have to go through the registration process elsewhere, such as the captive portal.

Host registered as a device

A host registered as a device can be displayed in the Host View or both the Host View and Inventory. Typically hosts registered as devices are items such as IP phones, security cameras, alarm systems or printers.

Settings

Field	Definitions
Register host to user	
User ID	ID of the user who owns this host. As you type a list of matching user IDs drops down. For example if you type ab, user IDs that start with ab are displayed. If the user ID does not exist in the database, but does exist in the directory used to authenticate users, the user is created at the same time. If the user does not exist either in the directory or in your database, you cannot save the host.

Field	Definitions
	If registering this host to a User exceeds the number of Allowed Hosts for that user, a message is displayed indicating that Allowed Hosts has been automatically incremented and the host is registered to the user.
Register host as device	
Create In	Indicates where the device should be displayed. Options include Host View or Host View and Inventory .
Container	If the host is created in both Host View and Inventory, you must choose a container to contain the host. Containers in Inventory are used to group devices.
General	
Role	Roles are attributes of hosts and users that can be used as filters in user/host profiles. If the host is registered to a user, there are two options for selecting the host role: • Use Role From User: Indicates that the host role is inherited from the registered user associated with the host. • Specify Role: Indicates that the host role is manually selected. This enables a drop-down list of possible roles from which you can choose. If the host is registered as a device in Inventory only, its role is used to control network access or can be used to apply a CLI configuration. For example, a CLI configuration could be used to reduce the baud rate of a device when it connects to the network.
Host Name	Name of the host being registered.
Hardware Type	Type of hardware such as Printer, Server or Workstation.
Serial Number	Serial number on the device. May be of assistance if the device is ever stolen.
Operating System	Operating system on the host, such as Windows or macOS. Only hosts with a valid operating system can be rescanned. Valid operating systems are Windows, Mac, and Linux.
Device Type	Indicates the type of device being disinterested registering a host to a user this field defaults to Registered Host With Owner. It could also be set to a gaming or mobile device. When registering as a device, this might be set to devices that are not typically associated with an owner, such as a printer or an alarm system. An icon representing the device selected displays beside the Device Type field. If the device is an access point and you register it in Host View, it is removed from the Host View and moved to Inventory after the first poll. It is also removed from the Concurrent License count once it is recognized as an Access Point.
Notes	Free form notes entered by the Administrator.
Security and Access Attribute Value	This value can be included in a filter when determining the Security Policy that should scan this host when it connects to the network. If a directory is in use and a user is associated with this host, the value comes from the directory when it is synchronized with the database. Otherwise the value can be entered manually.
Adapters	Lists the adapters or network interfaces that exist on this host. By listing all adapter's on the host here, you establish that these adapters are siblings. Number of adapters per host is limited to five.

Field	Definitions
	• Physical Address: MAC address of the adapter • Media Type: Indicates whether the adapter is wired or wireless.

Edit adapters

1. Go to the **Adapter** section of **Add or Modify Host**.
 - a. To add an adapter: Click **Add** and provide the **Physical Address** and the **Media Type**, such as wired or wireless.
 - b. To modify an adapter: Select an adapter and click **Modify**. Change the **Media Type** as needed. To change the **Physical Address**, you must delete the adapter and add it again.
 - c. To delete an adapter: Click on the adapter to select it and click **Delete**.
2. Click **OK** to save.



The number of adapters per host is limited to five.

View hosts and ports

1. Select Users & Hosts > Manage Hosts and Ports.
2. Click the appropriate host group and then click **Apply**.
3. A list of hosts contained in the selected group is displayed. The host information shown includes Status, Name, IP address, Description of the device and port where the host is connected, and On/Off control for the port.
4. Click the hostname to view the [Properties on page 221](#).
5. Click the Description to view the [Port properties on page 360](#).
6. Click **On** or **Off** to turn the port on or off.
7. Click **Apply** if any changes are made to the On/Off status of the port.

View and manage ports

1. Select Users & Hosts > Manage Hosts and Ports.
2. Click a port group and then click **Apply**.
3. A list of ports contained in the selected group is displayed. The port information shown includes Status, Description of the port, Name of the connected host (if any), and On/Off control for the port.
4. Click the **Status** icon to view the Connection details for the port.
5. Click the **Description** to view the [Port properties on page 360](#).
6. Click **On** or **Off** to turn the port on or off.
7. Click **Apply** if any changes are made to the On/Off status of the port.

Send message

FortiNAC has the ability to send SMS messages to administrators, guests or users. These messages are used to provide guests with user names and passwords, to notify administrators when an alarm has been triggered or to notify a user when an alarm has been triggered based on his host. FortiNAC sends SMS messages by sending email to a mobile phone number through a special email address provided by the mobile provider. For example, if you have a guest who is a Verizon Wireless customer and you need to send that guest an SMS message, the message is sent to xxxxxxxxx@vtext.com (where xxxxxxxxxx is the guest's cell phone number).



Both the Mobile Number and Mobile Provider must be entered into the guest, administrator or user record. SMS messages are sent via email. Without provider information FortiNAC cannot send SMS messages.



Long SMS messages might be divided up into multiple messages or truncated depending on how the Mobile Provider and the mobile telephone process long messages.

Implementation

To enable the SMS messaging feature you must configure the following:

Prerequisites

- Configure a connection to an out bound email server to send your SMS messages. See [Email/SMS/Email settings on page 937](#) for instructions.
- Review the list of mobile providers. Enable the providers that should be available to assign to guests, users, and administrators. The list is long so you may not want to enable them all. Add any providers that are not included in the list. Providers can be modified as needed. See [SMTP SMS Gateway](#).

SMS for guests

- Modify your current guest templates or create new ones to include **Send SMS message** as an option. Two data fields have been added to the Data Fields tab on the Add/Modify Template dialog to accommodate Mobile Number and Mobile Provider. Make sure you do not remove these fields or guests will not have a place to provide their mobile information when they register. See [Create templates on page 167](#).
- If you have existing guests that you would like to send messages to you must delete their guest records and recreate them using a template that has the Send SMS option enabled. Make sure to add Mobile Number and Mobile Provider for these guests.
- When guest accounts are created, you have the option to select one or more accounts from the list and send those guests an email and/or an SMS message containing their user name and password. See [Provide login information on page 164](#).

This is also true if you have set up a Kiosk for guests to create their own accounts. Guests can send themselves an SMS message with their credentials. To set up a Kiosk see [Using a kiosk on page 185](#).

If you have implemented Guest Self Registration and included **Send SMS message** in the template for those guests, guests can receive login credentials via SMS. See [Guest self registration on page 188](#).

- Mapping events to alarms and setting an SMS user notification action allows FortiNAC to send an SMS message to a guest. For example, if you want to send guests a message when their host is marked at risk and their network access is disabled, you can map the Host At Risk event to an alarm and send a message. The guest account must be associated with a template that has Send SMS enabled and the guest must have a Mobile Number and Provider entered on the Add/Modify User dialog. See [Add or modify alarm mapping on page 787](#).

SMS for administrators

- Add a Mobile phone number and Mobile provider to each administrator that should receive SMS messages. See [Add an administrator on page 121](#). This information can also be added by exporting administrators and re-importing them with their Mobile information. See [Import an administrator on page 109](#).
- Administrators that should receive SMS messages based on alarm mappings must be in one or more Administrator groups. Add administrators to the appropriate Administrator groups either from the Groups View or from the administrators view. See [Group membership on page 151](#).
- Mapping events to alarms, enabling options for notification and sending SMS messages to an Administrator group allows FortiNAC to send an SMS message to every administrator in the group. For example, if you want to send administrators a message if the database backup fails, map the Database Backup Failure event to an alarm and send an SMS message notifying administrators about the problem. See [Add or modify alarm mapping on page 787](#).

SMS for users

- Add a Mobile phone number and Mobile provider to each user that should receive SMS messages. See [Add or modify a user on page 202](#). This information can also be added by exporting Users and re-importing them with their Mobile information. See [Import hosts, users or devices on page 102](#).
- Mapping events to alarms allows FortiNAC to send an SMS message to a user. For example, if you want to send a user a message if their host has been disabled, map the Host Disabled Success event to an alarm and send an SMS message notifying the user about the problem. See [Add or modify alarm mapping on page 787](#).

Send messages to hosts

Use the Send Message option on the Bookmarks menu to send a real-time message to all hosts. This provides a method for you to get a message directly to the desktop of the selected hosts.

User can send messages to hosts with the Persistent Agent or Mobile Agent installed.

1. Select **Users & Hosts > Send Message**.
2. Click **All Hosts** to send the message to all hosts, or click **Group** and select a group of hosts to receive the message.
The message is sent only to the members of the selected group. Hosts who register and are assigned to the group after the message is sent will not receive the message, even if the message is still active.
3. Enter the message in the **Message** block.
4. If desired, enter a **Web Address** that will be sent as part of the message. Make sure the web address includes the http:// or ftp:// or other information. The page must also be in a location that the host(s) can access from their current VLAN, such as Remediation, Quarantine, Dead End, or other.
5. Click the radio button next to a **Message Lifetime** option and enter the information.
The server can only send messages to hosts with which it is communicating. If you have entered an expiration date and time, hosts who connect or communicate before that date and time also receive the message.

Message Lifetime Options	Description
Expires after sending to currently connected hosts	The message expires immediately after it has been sent.
Expires after	The message expires after the specified amount of time. Enter a number and select the timeframe of Minutes, Days, or Hours. The message remains active on the server for the selected timeframe. The server sends the message the next time it communicates with a host as long as communication occurs before the message expires.
Expires at	The message expires on the specified date and time. The format is MM/DD/YY hh:mm AM/PM. The message remains active on the server until the specified date and time. The server sends the message the next time it communicates with a host as long as communication occurs before the message expires.

6. Click **Submit**.

Network

Inventory	289

Inventory

Inventory provides an overview of the managed network. To access the Inventory, select **Network > Inventory**.

The Inventory tree is displayed in the left frame. It consists of FortiNAC and user-created containers. User-created containers contain managed network devices. Device icons displayed in the tree change to red if contact is lost. See [Inventory tree contact status on page 292](#). See [Icons on page 44](#) for a description of the icons.

The right pane displays a tabbed view with tabs for containers, devices, ports, and SSIDs, depending on the selection in the tree. For example, if a container is selected, tabs for devices, ports, and SSIDs are displayed.

Options

The right-click menu contains the following options based on the selected icon. When you select an item in the tree, the menu shows options specific to the selection.

Icon	Definition	Right-Click Options
 Find	Opens a search field above the Inventory Tree. Search for containers or devices by name, IP address or Physical address. See Find containers or devices on page 41 .	
 Customer	Represents the organization. When selected, a tabbed view is displayed in the right pane with tabs for Containers, Devices, Ports and SSIDs. Pingable devices are not displayed in the tabs on the right only in the tree.	• Add Container: Create a new container • Control Access Network Summary: Status of the access control groups for containers and devices • Import Port Descriptions: Import Port descriptions • Rename: Modify customer name
 Container	Containers allow logical grouping of network devices. When selected, a tabbed view is displayed in the right pane with tabs for Devices, Ports and SSIDs.	• Add Device: Add an SNMP enabled device to the selected container. • Add Pingable Device: Add a pingable device to the selected container. • Convert Pingables To Hosts: Convert all Non-SNMP devices in the container to Hosts. • Delete: Deletes the selected item • Start Discovery: Discovers SNMP enabled devices on your network and

Icon	Definition	Right-Click Options
Device	Represents individual network devices. When selected, a tabbed View is displayed in the right pane with tabs for Ports, Element, System, Polling, Credentials and, if applicable, SSIDs. If the device is a pingable, device properties are displayed in the right pane. Hosts that are displayed in Host View and Inventory are not shown in the right pane on the Devices tab because they are managed in Host View. You can display these hosts by clicking View in Host View.	adds them to the selected container • Modify: Modify the container name • Convert To Host: Convert a Non-SNMP device to a host. • Delete: Deletes the selected item • Group Membership: View Groups associated with this device • Local Mgmt (HTTP): Open an HTTP interface for local management of the device. Device must support local management. • Move To Container: Move selected device to a different container. • Network Access/VLANs: Modify Device Values, Summary, and Update Current & Default Values • Poll For Contact Status: Poll the device immediately instead of waiting for scheduled Poll. • Poll for L2 (Hosts) Info: Read the host information on the selected device and update the Ports tab. • Ports and Hosts: Display VLAN (Current and Default) and Host (Name and IP) information for each port on the device. • Properties: Provide detailed information about the device and allow some configuration. • Show Audit Log: Opens the admin auditing log showing all changes made to the selected item. • Modify: Edit contact and communication settings for the device. • Resync Interfaces: Update interface information for the device. • Role Membership: View associated roles. • Update Device Mappings: Assign a device type to an unknown SNMP device, allowing it to be managed. • Device Specific: Global Model Configuration, Model Configuration, Running Configuration, and Secure /Static Ports

Icon	Definition	Right-Click Options
		• Select Device In Tree: Highlights the non-SNMP device in the Inventory Tree and displays device properties in the right pane. Device Specific options vary depending on the device type.
Port	Ports cannot be selected in the tree, only from the Ports tab in the right pane.	• Connection Details: Opens a new view with information about hosts or users connected to the selected port • Group Membership: View or modify port groups containing selected port • Port Changes: Opens Port Changes View detailing changes to the selected port such as VLAN changes or CLI configurations applied. • Port Properties: Opens Port Properties, with current port settings and status • Role Membership: Displays list of roles that contain the selected port • Select Device In Tree: Highlights the device associated with the selected port in the Inventory Tree.
SSID	SSIDs cannot be selected in the tree, only from the SSIDs tab in the right pane.	• Properties: Opens the SSID Properties dialog with current settings • Group Membership: Displays list of groups that contain the selected SSID • Select Device In Tree: Highlights the device associated with the selected SSID in the Inventory Tree
Virtualized Devices	Virtualized Devices can be found from the Virtualized Devices tab in the right pane in the top-level on Inventory as well as each container. Supports multi-selecting VDOMs to launch Set Model Configuration.	• Model Configuration: Opens a new window with settings to configure the Model Configurations for the VDOM model • Add Virtualized Devices to Groups: Select or create groups to add Virtual Devices too. • Set Model Configuration: Opens a new view to set model configurations for the VDOMs with more details.

Inventory tree contact status

The tree in the left hand frame of the Inventory displays a list of network devices that are managed by FortiNAC, such as switches or routers. In addition to devices that provide network services, FortiNAC can manage pingable devices, such as alarm systems or printers.

Devices Displayed in Inventory Only

If FortiNAC cannot contact a device, a red box is displayed around the icon for the device and also around the icon for the Container used to group devices. The red icons in the Inventory tree indicate that the device has not responded to periodic ping requests sent by FortiNAC. Note there are circumstances in which devices are in contact with FortiNAC, but due to their configuration, they will not respond to a ping.

Directory servers communicate with FortiNAC via LDAP. The Inventory may turn the directory icon red even though the two are communicating. To prevent this, enable ping on the directory server.

See [Poll for contact status](#) for settings and additional details.

Devices Displayed in Both Host View and Inventory

These devices are managed by the Host View. The Host View does not use ping as a method to verify the connection between FortiNAC and the device. The Host View relies on L2 polling of the switch to which each device is connected to determine if the device is still connected and in contact with FortiNAC.

In the Inventory tree, the icons for devices managed in Host View will turn red if the device has not had any activity on the port to which it is connected for some time. This would eventually cause the MAC address of the device to be removed from the forwarding table of the switch. Depending on the device, you may want to manage it only in the Inventory. This prevents the icon from turning red indicating that contact with the device has been lost.

See [Icons on page 44](#) for status icon definitions.

Network summary

Displays the access status of the containers and devices on the network. Enforced indicates that access control is enforced on the container or device. For example, hosts connecting to a device in the registration access control group are forced to register. Not Enforced indicates that no ports on the device or container are in the access control group.

Percentage Enforced indicates the percentage of ports that are in the selected access control group. For example, if a switch has 10 ports, and % Enforced displays 80%, then 8 of the 10 ports for that switch are an access control group, such as Registration. Unregistered hosts connecting to one of the 8 ports would be forced to register.

If a device group has 5 switches, and % Enforced for the group displays 20%, then one of the 5 switches in the device group has some ports in the access control group selected.

1. Click **Network > Inventory**.
2. Right-click the **Customer** icon.
3. In the drop-down list, select **Control Access Network Summary**. This view shows all of the containers and devices on the network and their status for each system access group type.
4. Click in the **Type** field to select a different system access group. Options include: authentication, registration, remediation, dead end, and role-based access.
5. If there is a container, a device within a container, or device whose status is **Not Enforced**, use **Topology** and **Control Access** to modify their status.

Customer icon

The Customer icon in the Topology represents the organization. Select this icon to display tabs for Containers, Devices, Ports and SSIDs in the right frame. All Containers, Devices, Ports and SSIDs in the database can be accessed from here. Right-click on **Customer** to add containers, import port description data, and modify the customer name. Click **Find** to locate

See [Import port descriptions on page 116](#) and for additional information on those features.

When FortiNAC is installed, the Customer node in the Topology is listed as Customer. See [Rename the customer icon on page 295](#) for instructions on entering a new .

Settings

Field	Definition
Containers Tab	When Customer or Node is selected, the Containers tab is displayed with a list of all Containers in the database. Containers are also displayed in the tree under Customer. See Containers on page 296. Selecting a container from the Containers tab or from the tree provides you with the same set of right-click options. Add a container by right-clicking Customer or by selecting Add on the Containers tab. See Configure container for devices on page 297.
Devices Tab	When Customer or Node is selected, the Devices tab is displayed with a list of all Devices in the database. Devices are also displayed in the tree under the Container in which they reside. See Device view on page 314. Hosts that are displayed both in Host View and Topology are not displayed in the table of devices because they are managed in the Host View. They are displayed in the tree. Selecting a device from the Devices tab or from the tree provides you with the same set of right-click options. Add a device by right-clicking the Container Icon or by selecting Add on the Devices tab.
Ports Tab	When Customer or Node is selected, the Ports tab is displayed with a list of all Ports in the database. Ports are read from devices and cannot be added manually. See Ports view on page 354.
SSIDs Tab	When Customer or Node is selected, the SSIDs tab is displayed with a list of all SSIDs in the database. SSIDs are read from devices and cannot be added manually. See SSID view on page 365.
Right click options	
Add Container	Adds a new container to the database which is displayed in the tree. For additional information, see Configure container for devices on page 297.
Control Access Network Summary	Displays the control access enforcement status of all devices on the network. See Network summary on page 292.

Field	Definition
Import Port Descriptions	Import port descriptions into the FortiNAC Server and FortiNAC Control Server appliances from a .csv text file containing the comma separated values. See Import port descriptions on page 116 .
Rename	Modify the name of Customer. See Rename the customer icon on page 295 .

Configure container for devices

Containers are similar to folders and are used to group devices within your FortiNAC database. The Containers view also has a status column. As devices for a container are being discovered by FortiNAC the status of that process is displayed in the Status column. You must click **Refresh** at the top of the window to update the status.

When you delete a container, all associated devices are also deleted. To avoid this issue move your devices to a new container first, then delete the unwanted container.

Add a container

1. Select **Containers**.
2. On the Containers panel click **Add**.
3. Enter the Container Name and click **OK**.
4. Select the **Set as Default Wireless AP Location** check box to specify that the container is the default container where Wireless APs will be added. This will occur if there is no alternative AP location specified on the wireless device's model configuration view.

Modify a container

1. Select **Containers**.
2. On the Containers panel, select the container to be modified.
3. Click **Modify**.
4. Edit the name and click **OK**.
5. Select the **Set as Default Wireless AP Location** check box to specify that the container is the default container where Wireless APs will be added. This will occur if there is no alternative AP location specified on the wireless device's model configuration view.

Delete a container

1. Select **Containers**.
2. In the Containers panel select the Container to be removed.
3. Click **Delete**.

Note: Containers can be used in Device Profiling rules. See <https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/29753/adding-a-rule>

- If container is used in the Methods tab of a DPC rule, the container can be deleted. If deleted, FortiNAC removes the container from the DPC rule.
- If container is used in the General tab under Registration Settings, it cannot be deleted without removing the container from the DPC rule first. Otherwise, FortiNAC will display a message stating the container is currently

associated with a Device Profiling Rule.

Rename the customer icon

1. Click **Network > Inventory**.
2. Right-click **Customer** and select **Rename**.
3. Enter a new name.
4. Click **OK**.

Containers

Containers contains a modifiable list of containers for network devices. These containers provide a mechanism for you to logically group your devices. For example, you might make a container for switches and another for routers. You could make a separate container for each building that connects to your network or containers could represent departments in your business. If new devices have been connected to your network but have not been added to the device list, use **Start Discovery** to add them. From containers, you can add, modify or delete containers.

Deleting a container deletes the devices it contains. Move the devices to another container before deleting the selected container.

Settings

Field	Definition
IP Ranges	Range of IP addresses within which the discovery process searches for devices.
Discovery Status	Status of the device discovery process for the selected container. To update this field click Refresh at the top of the window.
SNMP Devices	Number of devices that are managed via SNMP within the selected container.
All Devices	Total number of devices within the selected container. Included both SNMP and non-SNMP devices.
Container	Name of the container. Containers are user-defined folders or groups for devices. Used to group devices by building or type.

Right-click menu options

Delete	Deletes the selected container.
Modify	Opens the Modify Container dialog for the selected container.
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746 .
 You must have permission to view the admin auditing log. See Add an administrator profile on page 139.	
Start Discovery	Searches the network based on user specified IP ranges and determines what SNMP enabled devices exist on the network. Once a device is discovered, FortiNAC creates a model for the device in the database and places the device in the Network Devices list. See Discovery on page 311 .
Cancel Discovery	Cancels the device discovery process for the selected container.
Discovery Results	Displays the results of the network scan used to discover devices in a separate Results View for the selected container. See Discovery results on page 313 .

Configure container for devices

Containers are similar to folders and are used to group devices within your FortiNAC database. The Containers view also has a status column. As devices for a container are being discovered by FortiNAC the status of that process is displayed in the Status column. You must click **Refresh** at the top of the window to update the status.

When you delete a container, all associated devices are also deleted. To avoid this issue move your devices to a new container first, then delete the unwanted container.

Add a container

1. Select **Containers**.
2. On the Containers panel click **Add**.
3. Enter the Container Name and click **OK**.
4. Select the **Set as Default Wireless AP Location** check box to specify that the container is the default container where Wireless APs will be added. This will occur if there is no alternative AP location specified on the wireless device's model configuration view.

Modify a container

1. Select **Containers**.
2. On the Containers panel, select the container to be modified.
3. Click **Modify**.
4. Edit the name and click **OK**.
5. Select the **Set as Default Wireless AP Location** check box to specify that the container is the default container where Wireless APs will be added. This will occur if there is no alternative AP location specified on the wireless device's model configuration view.

Delete a container

1. Select **Containers**.
2. In the Containers panel select the Container to be removed.
3. Click **Delete**.

Note: Containers can be used in Device Profiling rules. See <https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/29753/adding-a-rule>

- If container is used in the Methods tab of a DPC rule, the container can be deleted. If deleted, FortiNAC removes the container from the DPC rule.
- If container is used in the General tab under Registration Settings, it cannot be deleted without removing the container from the DPC rule first. Otherwise, FortiNAC will display a message stating the container is currently associated with a Device Profiling Rule.

Container icon

Containers are logical groups that are used to organize network devices. See [Configure container for devices on page 297](#) for more information. Click the Container icon to manually add, delete, and automatically discover devices, and to view and edit device properties.



A device must be given a unique name in order to appear in Inventory. You cannot add devices with duplicate names.



Any device you add to a container must be reachable by IP through ICMP/Ping and then with the SNMP v1 or v3 credentials. Check firewall settings to determine whether the device is reachable prior to adding the device to a container. Make sure ICMP is enabled on the network.

Network devices should have static IP addresses or dynamic IP addresses that are reserved. Once a device that provides network services had been identified in FortiNAC there is no mechanism to automatically update the IP address for that device if there is a change. If the IP address on the device itself is changed, the device appears in FortiNAC to be offline or to have a communication error.

When a Container is selected in the Inventory, the panel on the right displays Devices, Ports and SSIDs tabs. These contain lists of every device and every port that reside within the selected container. Hosts that display both in Host View and Inventory are not included in the Devices tab because they are managed through the Host View, and are indicated by the number of host devices not shown.

The title bar of the Devices panel shows the number of devices Displayed, Total Devices in the database and Host Devices that are not shown. The view in Host View link allows you to display the hosts that are managed in Host View.

To see host devices, expand the appropriate Container in the tree. Hover over an item in the tree to display the associated tool tip. The tool tip indicates whether the item is a Host or a Network Device.

Settings

Field	Definition
Devices Tab	When Customer or Node is selected, the Devices tab is displayed with a list of all Devices in the database. Devices are also displayed in the tree under the Container in which they reside. See Device view on page 314. Hosts that are displayed both in Host View and Inventory are not displayed in the table of devices because they are managed in the Host View. They are displayed in the tree. Click the View in Host View link to display the hosts that are managed in Host View. Selecting a device from the Devices tab or from the tree provides you with the same set of right-click options. Add a device by right-clicking the Container icon or selecting Add on the Devices tab.
Ports Tab	When Customer or Node is selected, the Ports tab is displayed with a list of all Ports in the database. Ports are read from devices and cannot be added manually. See Ports view on page 354.
SSIDs Tab	When Customer or Node is selected, the SSIDs tab is displayed with a list of all SSIDs in the database. SSIDs are read from devices and cannot be added manually. See SSID view on page 365
Right click options	

Field	Definition
Add Device	Adds an SNMP device to the selected container. See Add or modify a device on page 299
Add Pingable Device	Adds hubs, IPS/IDS, printers, servers, wireless access points and other non-SNMP or pingable devices to a container. See Add or modify a pingable device on page 302 .
Convert Pingables To Hosts	Converts one or more selected non-SNMP or pingable devices to hosts. After conversion these devices are removed from Network Devices but do display both in the Inventory and the Host View. See Convert all pingables to hosts on page 310 . Wireless access points added as pingables cannot be converted to hosts.
Start Discovery	Searches the network based on user specified IP ranges and determines what SNMP enabled devices exist on the network. Once a device is discovered, FortiNAC creates a model for the device in the database and places the device in the Network Devices list. See Discovery on page 311 .

Add or modify a device



FortiNAC-OS Requirement: "snmp" option must be included in the "set allowaccess" command. See [Open ports](#) for details.

You can manually add devices to a container. This process adds a single SNMP-enabled device at a time. Devices may be configured for SNMPv1 or SNMPv3 communication.



A device must be given a unique name in order to appear in Inventory. You cannot add devices with duplicate names.



If your device has multiple interfaces, each with a different IP address that is configured with its own SNMP settings, multiple representations of the same device will be added to FortiNAC. FortiNAC does not consolidate the duplicates in this case.

1. Click **Network > Inventory**.
2. Select the Container icon.
3. Right-click a container and select **Add Device** or right-click on a device in the Devices Tab and select **Modify**.
4. Click in the **Add To Container** field and select a container for this device. If the container you need does not exist, click the **New** icon and add the container first.
5. Enter the **IP address** of the device.
6. Select an **SNMP** protocol.
For SNMPv1 communication, enter the security string to use when communicating with the device.



If the device has multiple security strings, enter only the Read/Write security string. This is the string that will ensure that FortiNAC has the ability to control the device.

For **SNMPv3** communication enter the **User Name**, select the **Authentication Protocol**, and then enter the **Authentication Password** you used when you configured the device. For SNMPv3-AuthPriv, you must enter the **Privacy Protocol** and **Privacy Password**. These settings must match the corresponding settings on the device you are adding.

Settings

Field	Definition
API Key	The API key that generated from FortiGate that will be used in communication between FortiGate and FortiNAC.
Port	Enter the FortiGate HTTPS port number.
SNMP Protocol	Available options are AuthPriv or AuthNo Priv.
User Name	User Name for access to the device. Recommended but not required.
Authentication Protocol	Available options are: • MD5 • SHA1 • SHA224

Field	Definition
	• SHA256 • SHA384 • SHA512 (Recommended)
Authentication Password	Specify password to match what the device is using.
Privacy Protocol	Available options are: • DES • Triple DES • AES-128 • AES-192 • AES-256 (Recommended) • AES-192 Cisco • AES-256 Cisco
Privacy Password	Specify password to match what the device is using. Note: Ensure that passwords are at least 8 characters in length. Please note that longer passwords with repetitive strings may result in exactly the same key. For example, a password 'fortfort' will result in exactly the same key as password 'fortfortfort'.

If the device is configured for AuthPriv, the Authentication password, Privacy Protocol and Privacy password are required. If the device is configured for AuthNoPriv, only the Authentication password is required.

In the **CLI Settings** section, enter the Username, Passwords and Protocol for CLI access to this device. FortiNAC requires CLI access to manage hosts on the device.

CLI settings

Field	Definition
User Name	User name used to log on to the device for configuration. The user account must have the appropriate permissions configured on the device. For network devices using API credentials, the User Name is the serial number of the appliance.
Password	Password required to configure the device. For network devices using API credentials, the Password is the REST API Key.
Enable Password	Enable password for the device, if applicable. Note: Version 8.7.2 and higher: Arista switches can be configured to require typing "enable" to enter enable mode, but no password is needed. For such configurations, populate this field with the # character.
Protocol Type	Protocol used for communication with the device. Options include: Telnet, SSH1 and SSH2.

7. Click **Validate Credentials** to test the CLI and SNMP credentials entered.

8. Click **OK**.

9. Go to the **Model Configuration** view for this device to complete the configuration. See [Model configuration on page 338](#) for instructions.

Add or modify a pingable device

Use the Add Pingable Device option to add hubs, IPS/IDS, printers, servers, wireless access points and other pingable devices to a container. The Physical Address (MAC) is required when creating pingable devices if the IP to MAC cannot be resolved when the ARP tables are read.



A device must be given a unique name in order to appear in Inventory. You cannot add devices with duplicate names.

1. Click **Network > Inventory**.
2. Select the **Container** icon.
3. Right-click a container and select **Add Pingable Device** or right-click on a pingable device in the **Devices** tab and select **Modify**.
4. From the drop-down menu select the **Container** where this device will be stored. You can use the icon next to the **Container** field to add a new container.
5. Use the tables below to create or modify the pingable device.
6. Click **OK**.

Element tab settings

Field	Definition
Container	Container in the Inventory where this device is stored.
Name	Name of the device
IP address	IP address of the device
Physical Address	The MAC address of the device. Appears in the view only when the device is a pingable.
Device Type	Select the device type from the drop-down list.
Incoming Events • Not Applicable • Syslog • Security Events <i>Available when Security Incidents is configured.</i>	When Syslog is selected, available syslog files appear that can be used by FortiNAC to parse information received from the external devices and generate an event. When Security Events is selected, available security event parsers appear that can be used by FortiNAC to parse information received from the external devices and generate a security event. See Security event parsers on page 970 .
SSO Agent	• Not Applicable • Custom Script • Palo Alto • RADIUS • iboss

Field	Definition
Custom Script	Displayed when Custom Script is selected in the SSO Agent field. Allows you to write and select a script that will integrate with a SSO Agent that is not currently supported.
Apply to Group	Select this check box to apply the Custom Script SSO options only to the selected Host group in the drop-down list. If you do not select the check box, the SSO options are applied to all Host groups.
RADIUS Accounting Port	Displayed when RADIUS is selected in the SSO Agent field. Port on the Fortinet Single Sign-On User Agent configured to receive RADIUS Accounting messages from external devices. This port must match the port configured in Fortinet.
RADIUS Secret	Displayed when RADIUS is selected in the SSO Agent field. Must match the RADIUS secret configured for FortiNAC in Fortinet.
Apply to Group	Select this check box to apply the RADIUS SSO options only to the selected Host group in the drop-down list. If you do not select the check box, the SSO options are applied to all Host groups.
XML API Port	Displayed when Palo Alto User Agent is selected in the SSO Agent field. Port on the Palo Alto User Agent configured to receive messages from external devices. This port must match the XML API port configured on the Palo Alto User Agent. See Add or modify the Palo Alto User-ID agent as a pingable on page 304 .
Domain Name	Displayed when Palo Alto User Agent is selected in the SSO Agent field. FQDN for your network users' domain. This is sent with the logged in user ID to Palo Alto.
Use Integrated Agent	When selected, FortiNAC will integrate with the firewall directly.
API Key	Displayed when the Use Integrated Agent check box is selected. Enter the API Key value. The key can be retrieved manually or by select Retrieve .
Apply to Group	Select this check box to apply the Palo Alto SSO options only to the selected Host group in the drop-down list. If you do not select the check box, the SSO options are applied to all Host groups.
iboss Port	Displayed when iboss is selected in the SSO Agent field. The iboss port is the iboss HTTP port that is used to talk to the iboss SSO agent. The iboss port is defined in the iboss SSO GUI.
iboss Key	Displayed when iboss is selected in the SSO Agent field. The iboss key is a security key used to talk to the iboss SSO agent. The iboss key is defined in the iboss SSO GUI.
iboss Domain	Displayed when iboss is selected in the SSO Agent field. The iboss Domain is a required field that allows the user to enter their Active Directory domain name.
Apply to Group	Select this check box to apply the iboss SSO options only to the selected Host group in the drop-down list. If you do not select the check box, the SSO options are applied to all Host groups.
Role	The Role for this device. Available roles appear in the drop-down list.
Description	Description of the device entered by the Administrator.
Note	User specified notes about the device.

Field	Definition
Contact Status Polling	Enable or disable contact status polling for the selected device.
Poll Interval	Determines how often the device should be polled for communication status. Time is stored in minutes.
Poll Now	Polls the device immediately for contact status.
Last Successful Poll	Date and time that the device was last polled successfully.
Last Attempted Poll	Date and time that the device was last polled.

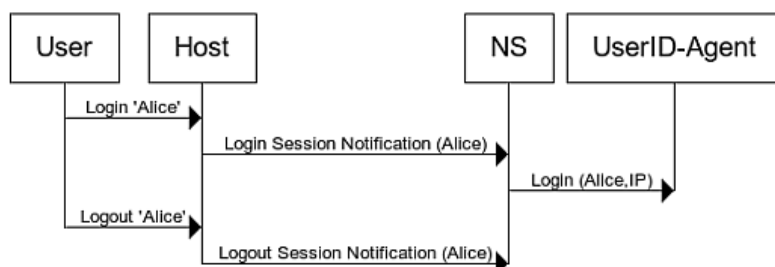
Details tab settings

Field	Definition
Host Name	Name of the device.
Department	Name of the department.
Owner	Name of the owner of the device.
Administrative Contact	Administrative contact person for the device.
Geographical Location	Geographical location of the device (for example, Res Hall A, Equipment Closet 1st Floor, Rack 2, Unit 3).
Business Purpose	Business purpose of the device.
BOOTP Address	IP address for the BOOTP Protocol.
Print Queue	Name of the print queue for the device.

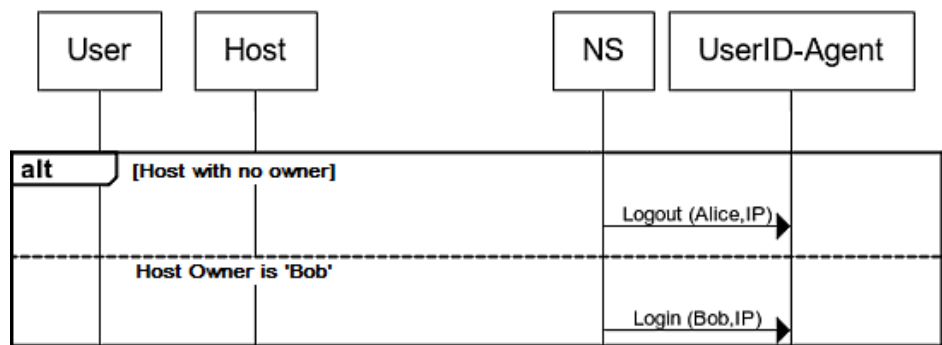
Add or modify the Palo Alto User-ID agent as a pingable

When the Palo Alto Networks User-ID agent is configured in FortiNAC as a pingable device, FortiNAC sends a message to Palo Alto Networks firewall each time a host connects to the network or the host IP address changes, such as when a host is moved from the Registration VLAN to a Production VLAN. A message is also sent when one user logs off a host and a new user logs on to that same host while the host is still on-line. All messages include user ID and IP address. This information identifies the user to Palo Alto Networks allowing it to apply user specific policies. There are several scenarios that generate messages to Palo Alto Networks, as described below and in the flow diagram:

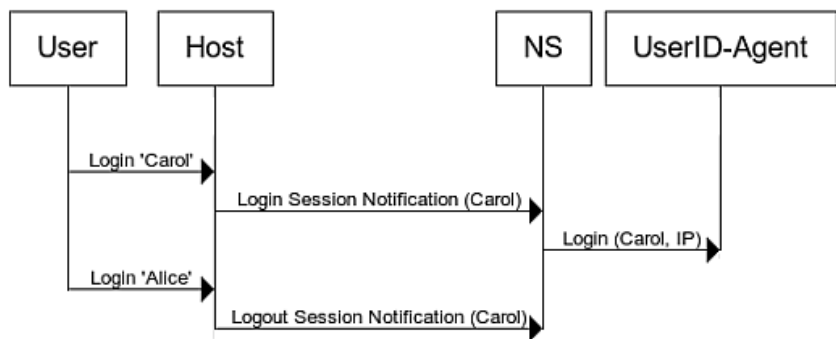
A host is registered to a specific user; the owner logs onto the network with the host. FortiNAC sends user ID and IP address.



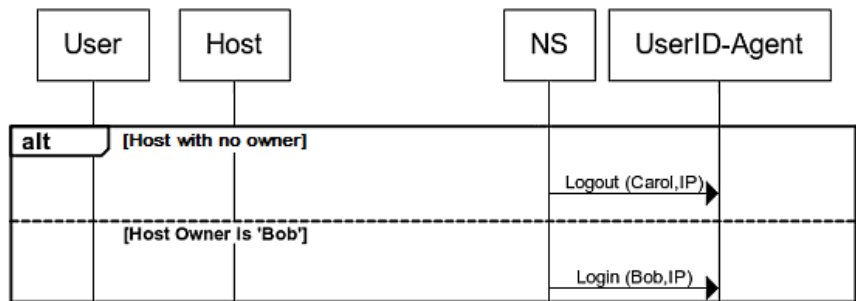
A host has no associated owner and is registered as a device; a user logs onto the network with this host. If this yields a logged on user, FortiNAC sends user ID and IP address.



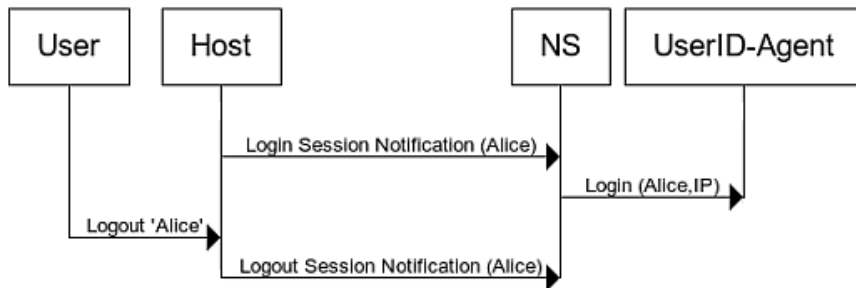
If a host is registered to a specific user, when a different user logs onto the host, that new user's user ID is sent to Palo Alto Networks with the host IP address.



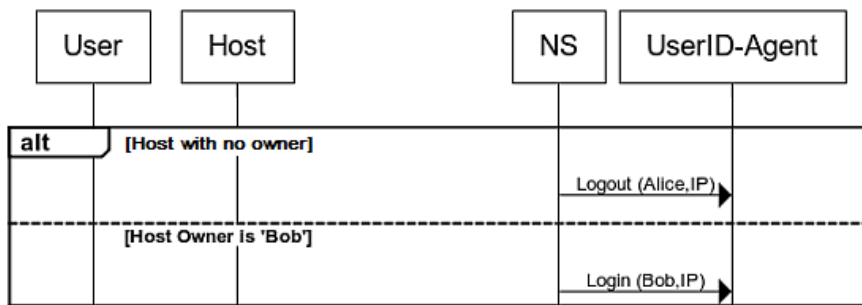
When a user who is not registered as the host's owner logs out of the host, the user ID of the host's owner is sent to Palo Alto Networks with the host IP address, even though the owner did not actually log onto the network.



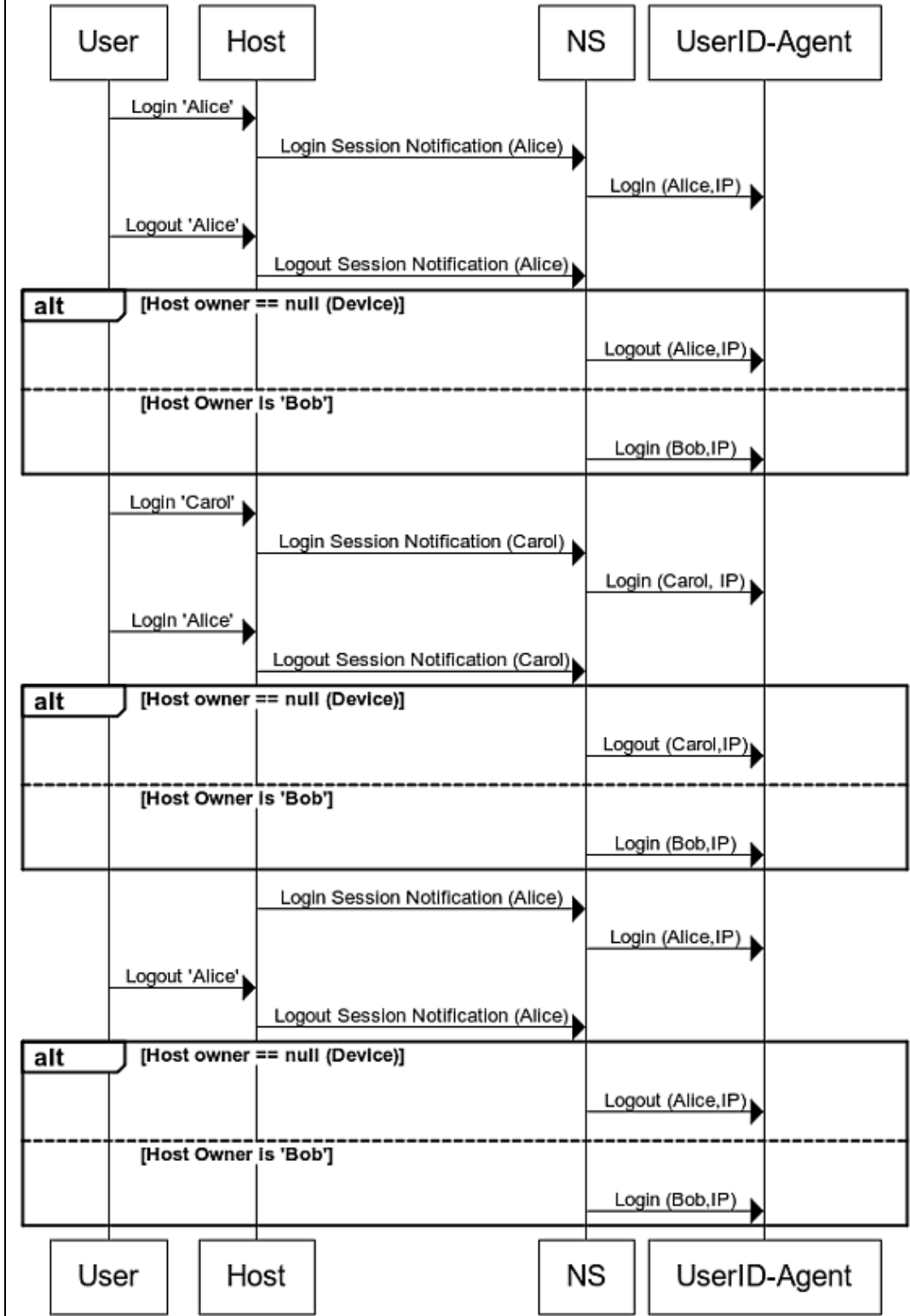
When a user logs out of a host that has no owner, FortiNAC notifies Palo Alto Networks that the user has logged out.



If a user is logged in remotely, such as through Remote Desktop, and there is no Persistent Agent installed on the host, login and logout information are not provided to Palo Alto Networks.



Network Sentry -> Palo Alto integration



Implementation

To integrate with the Palo Alto Networks User-ID agent you should be aware of and configure the following items:

Palo Alto Networks

- Palo Alto Networks firewall must be Version 4.0 or higher.
- Palo Alto Networks User-ID agent must be Version 4.0 or higher.
- For Palo Alto Windows User-ID agent versions prior to 7.0.4, the XML API must be enabled to allow communication with FortiNAC. In the Windows User-ID agent under **User Identification > Setup** make sure **Enable User-ID XML API** is set to **Yes**. This option is configured on the **Agent Setup** dialog under the **Agent Service** tab.



FortiNAC cannot integrate with Windows User-ID Agent versions 7.0.4 and higher because the Enable User-ID XML API option is not available.

FortiNAC

- To configure the integration of FortiNAC with the Windows User-ID Agent for Agent Versions prior to 7.0.4, do not select the **Use Integrated Agent** check box. Specify the **XML API Port** value to match the port you have configured the Windows User-ID agent to use. The agent uses port 5007 by default.
- FortiNAC cannot integrate with the Windows User-ID Agent Version 7.0.4 or later. If you cannot use an earlier version of the agent, you can instead configure FortiNAC to integrate with the firewall directly.
- If you are not using the Windows User-ID Agent and your firewall is version 6.0 or later, you must configure FortiNAC to integrate directly with the firewall. Select the **Use Integrated Agent** check box and enter port 443 in the **XML API Port** field. Enter the **API Key** value. The key can be retrieved manually or by selecting **Retrieve**.



Direct integration of FortiNAC with versions of the firewall prior to 6.0 is not supported.

-
- Hosts that will be affected by or managed by the Palo Alto Networks User-ID agent must have a logged-on User. If no user is associated with the host, only the IP address is sent to the Palo Alto Networks User Agent. The User Agent cannot apply a policy without a user ID. Registration methods such as the Persistent Agent, device profiler, or login scripts can be set to register hosts as devices, but then it is the user's login/logout that triggers that messages be sent from FortiNAC to Palo Alto.
 - Add the Palo Alto Networks User Agent as a pingable device in FortiNAC. See the instructions below for the steps.
 - FortiNAC and the Palo Alto Networks User Agent communicate via SSL. SSL certificates on the Palo Alto Networks User Agent Server are automatically imported into the .keystore file on your FortiNAC Control Server or Server.
 - In Event Management, the event **Communication Lost With Palo Alto User Agent** is automatically enabled. This event is generated when the Palo Alto Networks User Agent cannot be reached. The Palo Alto Networks User Agent is not being notified when hosts connect to the network, therefore, policies may not be applied. See [Enable and disable events on page 773](#) to disable the event if necessary.
 - In Event to Alarm Mappings, you can map the **Communication Lost With Palo Alto User Agent** event to an alarm if you wish to be notified when FortiNAC and the Palo Alto Networks User Agent are no longer communicating. See [Add or modify alarm mapping on page 787](#).

Add pingable

1. Click **Network > Inventory**.
2. Select the **Container** icon.
3. Right-click the container and select **Add Pingable Device**.
4. Use the table below to enter the data for the Palo Alto Networks User-ID agent.
5. Click **OK** to save.

Settings

Field	Definition
Element tab	
Container	Container in the Inventory where this device is stored.
Name	Name of the device
IP address	IP address of the device
Physical Address	The MAC address of the device. Appears in the view only when the device is a pingable.
Device Type	Lists all available device types. Select Firewall or Server.
Incoming Events	Lists the security appliances available when either Syslog or Security Events is selected. Select Not Applicable.
SSO Agent	The third party agent communicating with the same authentication credentials as FortiNAC, utilizing the ability to unify credentials across multiple products (e.g., Single Sign-On).
XML API Port	Displayed when Palo Alto User Agent is selected in the SSO Agent field. Port on the Palo Alto User Agent configured to receive messages from external devices. This port must match the XML API port configured on the Palo Alto User Agent. See Add or modify the Palo Alto User-ID agent as a pingable on page 304 .
Domain Name	Displayed when Palo Alto User Agent is selected in the SSO Agent field. FQDN for your network users' domain. This is sent with the logged in user ID to Palo Alto.
Use Integrated Agent	Allows you to integrate directly with the firewall when FortiNAC does not integrate with the Windows User-ID Agent.
API Key	The authorization key that allows a user to send user mapping data to the firewall. Can be retrieved from the firewall manually, or by providing the credentials for an administrator account on the firewall when you select Retrieve .
Apply to Group	Select this check box to apply the Palo Alto SSO options only to the selected Host group in the drop-down list. If you do not select the check box, the SSO options are applied to all Host groups.
Role	The Role for this device. Available roles appear in the drop-down list.
Description	Description of the device entered by the Administrator.

Field	Definition
Note	User specified notes about the device.
Contact Status Polling	Enable or disable contact status polling for the selected device.
Poll Interval	Determines how often the device should be polled for communication status. Time is stored in minutes.
Poll Now	Polls the device immediately for contact status.
Last Successful Poll	Date and time that the device was last polled successfully.
Last Attempted Poll	Date and time that the device was last polled.

Convert all pingables to hosts

Non-SNMP devices displayed in the Inventory can be converted to Hosts. These hosts display both in the Host and Inventory. Rogues that display in the Host View can be registered as devices in both Host View and Inventory. See [Register a host as a device on page 232](#).

Devices that are kept in the Host View have a connection history and can be associated with a user. Devices that are placed in the Inventory can be polled for their connection status. Devices that are not connected display in red on the Inventory. If the connection to the device fails, events and alarms can be configured to notify you that the device is no longer communicating.

There are certain repercussions when pingables are converted to hosts that should be taken into consideration:

- Converting a pingable device to a host causes that device to be subject to aging rules configured for hosts. Aging rules control the expiration and inactivity dates used to automatically remove hosts from the database. See [Aging out host or user records on page 241](#).
- When a device is converted to a host the IP address of that device is not propagated to the host record. The next L3 poll will add the IP address to the host record.

Wireless access points added as pingable devices cannot be converted to hosts.

Convert all pingables

1. Click **Network > Inventory**.
2. Select the **Container** icon.
3. Right-click a container and select **Convert Pingables To Hosts**. This option converts all non-SNMP devices to hosts and displays them both in Host View and Inventory.
4. Click **Yes** on the confirmation window.
5. Select **Users & Hosts > Hosts** and verify that the Pingable devices now display in Host View.

Convert one or more pingables from Inventory

1. Click **Network > Inventory**.
2. Expand the **Container** where the device is located.
3. Select the device to be converted. Hold down the **Ctrl** key to select multiple devices.
4. Right-click a device and select **Convert To Host**. This option converts the non-SNMP devices selected to hosts.

5. Click **Yes** on the confirmation window.
6. Select **Users & Hosts > Hosts** and verify that the pingable devices now display.

Convert one or more pingables from network devices view

1. Click **Network > Inventory**.
2. Make sure the filter is set to display the devices to be converted.
3. Select the device to be converted. Hold down the **Ctrl** key to select multiple devices.
4. Click **Convert To Host**. This option converts the non-SNMP devices selected to hosts.



The conversion skips any selected SNMP devices and warns you of the number of devices that were not converted.

5. Click **Yes** on the confirmation window.
6. The device is removed from the Network Devices window, but will display in Inventory and Host View.
7. Select **Users & Hosts > Hosts** and verify that the Pingable devices now display.

Discovery



FortiNAC-OS Requirement: "snmp" option must be included in the "set allowaccess" command. See [Open ports](#) for details.

FortiNAC can search the network based on IP ranges and determine what SNMP enabled devices exist on the network. Once a device is discovered, FortiNAC creates a model for the device in the database and places the device in the Network Devices list.

FortiNAC receives traps and communicates with devices through SNMPv1, SNMPv2, and SNMPv3.

When the **Use CDP** option on the **Discovery** window is enabled, FortiNAC queries devices about other connected devices on the network. If a device has this discovery protocol enabled it gathers and stores information about devices it manages and devices it can contact on the network. Enabling the **Cisco Discovery Protocol (CDP)** when adding search criteria for discovery allows FortiNAC to query devices for information about those secondary devices. For example, FortiNAC can query a device and discover routers and switches connected to the original device. FortiNAC can then query those secondary devices and so on, until the edge of the network is reached. Only devices with CDP enabled will respond to a CDP query.

When a discovery process is started for a particular container, the status of that process is displayed in the **Containers** view. Click **Refresh** on the **Containers** view to update the status periodically.

Note:

- Important: When adding IP ranges, the total number of IP addresses covered should not exceed 65,000 (example: range 1 + range 2 + range 3 = 65,000). Otherwise, the discovery may not complete.
- In large networks, discovery can take an extended amount of time.
- If a device has multiple interfaces, each with a different IP address that is configured with its own SNMP settings, multiple representations of the same device will be added to FortiNAC. FortiNAC does not consolidate the duplicates in this case.

- When configuring the device itself, use only letters, numbers and hyphens (-) in names for items within the device configuration, in security strings and in SNMP credentials. Other characters may prevent FortiNAC from reading the device configuration. For example, in many cases the # sign is interpreted by FortiNAC as a prompt. Cisco restricts the use of @ and #.

1. Go to **Network > Inventory > Customer > Containers**.
2. Select a Container that will be populated by the discovery process.
3. Click **Start Discovery** in the Containers panel.
4. The Discovery Settings window displays.
5. If you would like to search for devices using the Cisco Discovery Protocol, click the **Use CDP** check box to enable it.
6. On the IP Range tab, click **Add**.
7. Enter the **Starting** and **Ending IP addresses** of the range to be queried for new devices. If you selected **Use CDP**, only the starting IP address is required.
If you have an extensive network and you plan to use CDP, it is recommended that you limit the number of levels queried beyond the initial device. In large networks, discovery can take an extended amount of time and may cause delays. For information on limiting the depth of the CDP discovery see [Network device on page 910](#).
8. Add all of the IP ranges required.
9. Click **Next** or click the **SNMP Credentials** tab.
10. Under **SNMPv1 Security Strings**, enter the read/write security strings to use when communicating with the discovered devices. Click **Add** to add a security string. Select a security string and click **Delete** to remove it from the list.
11. Under SNMPv3 Credentials, click **Add** to enter the settings to use when communicating with the discovered devices.

Settings

Field	Definition
SNMP Protocol	Available options are AuthPriv or AuthNo Priv.
User Name	User Name for access to the device. Recommended but not required.
Authentication Protocol	Available options are: MD5 SHA1 (Recommended)
Authentication Password	Specify password to match what the device is using.
Privacy Protocol	Available options are: DES AES-128 (Recommended)
Privacy Password	Specify password to match what the device is using.



If the device is configured for AuthPriv, the authentication password, Privacy Protocol and Privacy password are required. If the device is configured for AuthNoPriv, only the authentication password is required.

12. Click **Next** or click the **CLI Credentials** tab.

13. Click **Add** to enter CLI Credentials for managing discovered devices.

Settings

Field	Definition
User Name	The user name used to log on to the device for configuration. This is for CLI access.  For devices using API credentials, enter the serial number for the appliance.
Password	The password required to configure the device. This is for CLI access.  For devices using API credentials, enter the REST API Key.
Enable Password	The enable password for the device. This is for CLI access. Depending on the configuration, you may not need both the password and the enable password. Note: Version 8.7.2 and higher: Arista switches can be configured to require typing "enable" to enter enable mode, but no password is needed. For such configurations, populate this field with the # character.
Protocol Type	Use Telnet, SSH1 or SSH2 to logon to the device for configuration.

14. Click **OK** to start the discovery process. The process runs in the background.
The status of a discovery task is displayed in the **Devices** header.
15. Click **Cancel Discovery** to cancel the discovery process.

Discovery results

Discovery Results displays a dialog with detailed information about the discovery process. Access Discovery Results from **Network > Inventory > Customer > Containers**.

Settings

Field	Definition
Device Address Range	Range of IP addresses selected and the total number of addresses within the range.
Devices Scanned	Number of devices within the IP address range that were scanned.
New Devices Found	Number of devices in the IP address range that were added to the database.
Scan Completed	Date and time that the discovery process finished scanning the network for devices.
SNMP Errors	List of IP addresses that were scanned but with which FortiNAC could not communicate via SNMP.

Field	Definition
CLI Errors	List of IP addresses that were scanned and with which FortiNAC was able to communicate via SNMP, but the CLI Credentials were incorrect.

Device view

When a Container is selected in the tree on the Topology, the Devices tab is displayed in the panel on the right. Devices can be hubs, pingables, printers, servers, or switches and have various management options, depending on the device type. To view these management options, select a device from the tree or the table and then right-click to view the drop-down menu.

Settings

Field	Definition
Status	Indicates whether or not communication has been established with the device. Displays either Established or Lost.
Name	Name of the selected device.
IP address	IP address of the selected device. IP addresses or Address Ranges are used to add or discover devices.
Physical Address	MAC address of the selected device.
Container	Container where the device resides. Containers are used to group devices.
Role	Displays the role assigned to this device. To modify the role go to Device Properties for this device. This field does not list the roles associated with this device through network device roles. To view role membership, right-click on the device in the Topology.
Notes	User specified notes about the device that are entered on the Device Properties view.
Raw Type	The OID of the device.
Device Type	Indicates the type of devices, such as switch, printer, router, etc.
Protocol	SNMP version used for the device, options include: SNMPv1, SNMPv3 and Pingable.
CLI Protocol	Communication method used to connect to the CLI of the device, options include: Telnet, SSH1 and SSH2.
Polling	Indicates whether polling is enabled or disabled and displays the polling interval.
Last Polled	Date and time the server last attempted to poll the device.
Last Polled Success	Date and time that the device was last polled successfully.
L2 Polling	Indicates whether L2 polling is enabled or disabled and displays the polling interval.
L2 Last Polled	Date and time the server last attempted a L2 poll of the device.
L2 Last Polled Success	Date and time of the last successful L2 poll.
L3 Polling	Indicates whether L3 polling is enabled or disabled and displays the polling interval.

Field	Definition
L3 Last Polled	Date and time the server last attempted a L3 poll of the device.
L3 Last Polled Success	Date and time of the last successful L3 poll.
CDP Polling	Indicates whether CDP polling is enabled or disabled for the device and displays the polling interval. Disabled (unsupported) displayed in this column, indicates that the first CDP poll was unsuccessful because CDP queries are not supported by the device or may not be configured on the device. If the device has ever been successfully polled for CDP, later unsuccessful polls are not interpreted as a problem with CDP on the device.
CDP Last Polled	Date and time the server last attempted a CDP poll of the device.
CDP Last Poll Success	Date and time of the last successful CDP poll.
Group	Filters the list of devices based on the group selected. Only devices that are members of the selected group display in the list.
Last Modified By	User name of the last user to modify the device.
Last Modified Date	Date and time of the last modification to this device.
Right click options	
Add	Add a SNMP device to the Topology, such as a switch. See Add or modify a device on page 299 .
Add Pingable	Add a pingable device to the Topology, such as an alarm system. See Add or modify a pingable device on page 302 .
Delete	Deletes the selected devices.
Modify Properties	Appears when multiple devices are selected. Allows you to modify device properties for multiple devices simultaneously. See Modify multiple device properties on page 329 .
Convert To Host	Converts one or more selected non-SNMP or pingable devices to hosts. After conversion these devices are removed from Network Devices but do display both in the Topology and the Host View. See Convert all pingables to hosts on page 310 . Wireless access points added as pingables cannot be converted to hosts.
Group Membership	Displays the device group membership, which allows you to view and modify the groups in which this device is a member. See Device group membership on page 318 . There is now a search bar and a collapse all tab for port groups.
Local Management (HTTP)	Opens a browser to manage the device through the web interface. This option may not be available for all devices.
Move To Container	Moves the selected devices to a different Container. See Move a device to a different container on page 319
Network Access/VLANS	Modify device and model values and display the current and default network access assignments stored in the FortiNAC model of that device. See Network access/VLANs on page 319 .

Field	Definition
Poll For Contact Status	Polls the selected devices immediately instead of waiting for the next scheduled poll. See Poll for contact status on page 322 .
Poll For L2 Hosts Info	Reads the host information on the selected device and updates the Ports tab in Topology. See Poll for L2 (hosts) information on page 323 .
Ports And Hosts	Displays VLAN (Current and Default) and Host (Name and IP) information for each port on the device. If the host name is unknown, the MAC address is displayed. See Ports and hosts on page 323 .
Properties	Displays the Properties View for the selected device. See Device properties on page 323 and Pingable device properties on page 329 .
Modify	Modify the selected device. See Add or modify a device on page 299 or Add or modify a pingable device on page 302 .
Resync Interfaces	Reads the interface information from a modeled device and updates FortiNAC's representation of that device. This information includes the interface's index, description, name, and status. See Resync interfaces .
Role Membership	Displays the list of roles in which the device is a member. See View role membership on page 332 .
Select Device In Tree	Locates the selected device in the tree on the right and highlights it.
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746 .
	 You must have permission to view the admin auditing log. See Add an administrator profile on page 139.
Show Events	If the Devices tab is selected, displays events for the selected device. If the Ports tab is selected, displays events for the selected port.
Update Device Mappings	Update device icon for the selected device when the device type is unknown and the icon is a question mark. See Update device mapping on page 333 .
Global Model Config	Opens the Global Model Configuration window to configure data for multiple devices of the same brand, such as passwords for communication with the device, VLANs, and RADIUS server information. See Global model configuration on page 344 .
Model Config	Opens model configuration for the selected device to configure data such as passwords for communication with the device, VLANs, and RADIUS server information. See Model configuration on page 338 .
Running Configuration	View the configuration running on the selected device (device dependent). This option is only available for some devices.
Static Port Configuration	Allows you to designate a specific port as a Dead-End VLAN and use that port to disable hosts. The MAC address of the disabled host is placed in a list on the device which indicates it only has permission to use the port designated as secure or static. See Secure port/static port overview on page 349 .

Delete a device

When a device is deleted the associated configuration is also removed.

1. Click **Network > Inventory**.
2. Expand the **container** where the device is located.
3. Select the device to be deleted.
4. Click **Edit > Delete** to remove the device from the container.

Replace a device using the same IP address

When adding a switch or router that will use the same IP address as the original device modeled in Inventory, the original model must be deleted from the database and a new model added. This ensures all internal mappings and other related files associated to that model are correct for the new device. Otherwise, unexpected behavior occurs.

Note: Deleting the model from FortiNAC removes all manual switch device and port groupings done on the switch model.

1. Review the model of the device to be replaced. Note or take screen captures of all configurations, including port and device group memberships. They will need to be re-entered later.
2. Ensure the new device is configured appropriately.
3. Once original device is decommissioned, delete the old device model. See [Delete a device](#).
4. Once the new device is on the network, add to Inventory using the appropriate credentials. See [Add or modify a device](#).
5. Configure device model using the settings recorded previously.

Convert devices to hosts

Non-SNMP devices displayed in the Inventory can be converted to Hosts. These hosts display both in the Host and Inventory. Rogues that display in the Host View can be registered as devices in both Host View and Inventory. See [Register a host as a device on page 232](#).

Devices that are kept in the Host View have a connection history and can be associated with a user. Devices that are placed in the Inventory can be polled for their connection status. Devices that are not connected display in red on the Inventory. If the connection to the device fails, events and alarms can be configured to notify you that the device is no longer communicating.

There are certain repercussions when pingables are converted to hosts that should be taken into consideration.

- Converting a pingable device to a host causes that device to be subject to aging rules configured for hosts. Aging rules control the expiration and inactivity dates used to automatically remove hosts from the database. See [Aging out host or user records on page 241](#).
- When a device is converted to a host the IP address of that device is not propagated to the host record. The next L3 poll will add the IP address to the host record.



Wireless Access Points added as pingable devices cannot be converted to hosts.

Convert all pingables in a container

1. Click **Network > Inventory**.
2. Select the **Container** icon.
3. Right-click a container and select **Convert Pingables To Hosts**. This option converts all non-SNMP devices to hosts and displays them both in Host View and Inventory.
4. Click **Yes** on the confirmation window.
5. Select **Users & Hosts > Hosts** and verify that the pingable devices now display in Host View.

Convert from Inventory

1. Click **Network > Inventory**.
2. Expand the **container** where the device is located.
3. Select the device to be converted. Hold down the **Ctrl** key to select multiple devices.
4. Right-click a device and select **Convert To Host**. This option converts the non-SNMP devices selected to hosts.
5. Click **Yes** on the confirmation window.
6. Select **Users & Hosts > Hosts** and verify that the pingable devices now display in Host View.

Convert from Network Devices view

1. Click **Network > Inventory**.
2. Make sure the filter is set to display the devices to be converted.
3. Select the device to be converted. Hold down the **Ctrl** key to select multiple devices.
4. Click **Convert To Host**. This option converts the non-SNMP devices selected to hosts.
5. Click **Yes** on the confirmation window.
6. The device is removed from the **Network Devices** window, but will display in Inventory and Host View.
7. Select **Users & Hosts > Hosts** and verify that the pingable devices now display in Host View.

Device group membership

Devices on your network can belong to groups. Group membership can be viewed from the Groups View window or by selecting the device in the Inventory.

1. Click **Network > Inventory**.
2. Expand the **Container** where the device is located.
3. On the Devices panel on the right, right-click on a device and select **Group Membership**.
4. Check marks indicate that the device is a member of the group.
5. **To add the device to a group**, click the box next to the group name and then click **OK**.
6. **To remove the device from a group**, click to uncheck the box next to the group name and then click **OK**.
7. Click **OK** to save your group selections.

If an item is placed in a subgroup, it can only be removed when viewing the membership of that subgroup. It cannot be removed from the parent group containing the subgroup.

For example, the L2 network devices group contains the wired devices and wireless devices subgroups. The wired devices subgroup contains four 3COM switches. The wireless devices subgroup contains two Cisco switches. The L2

network devices group membership list shows all six switches, but to remove one of the 3COM switches you must go to the wired devices membership list.

Local management

Use the Local Management option to open a browser and manage the device through the web interface. This option may not be available, depending on the device.

1. Click **Network > Inventory**.
2. Expand the **Container** where the device is located.
3. Right-click the device and select **Local Management (HTTP)**.
4. A browser window opens and displays the login window for this device.

Move a device to a different container

1. Click **Network > Inventory**.
2. Expand the **Container** where the device is located.
3. Right-click on the device to be moved.
4. Select **Move To Container**.
5. Select the container where the device will be located.
6. Click **OK**. The device is now listed in the Inventory under container.

Network access/VLANs

Use this option to modify device and model values and to display the current and default network access assignments stored in the FortiNAC model of that device. Network access could be through VLANs/Roles, CLI configurations, or VPN groups, depending on the device type. In the following discussion, the term **VLANs** refers to any of the network access types.

- The current VLANs are read from the device in the following situations:
- When you click Read VLANs in VLAN Summary view of the device.
- When the first trap (link up, link down, or cold start) is received after the device is added to the Inventory.
- When the first trap (link up, link down or cold start) is received after regaining contact with the device.
- When the first trap (link up, link down, or cold start) is received after starting up FortiNAC.



If you have not yet supplied the telnet or SSH parameters, FortiNAC can not retrieve the VLANs.

The VLANs option allows you to force a read of the current values from the device, edit the model's current values, and modify the default VLAN values.

Important: Manually changing VLANs should be done through the Administration UI instead of the switch itself. For details, see article Best practice for manually changing VLANs on managed switches

The modified default values are stored in the FortiNAC database but do not perform a write memory to the boot configuration for switch vendors whose switches support running and boot configurations.



The FortiNAC default VLAN is the VLAN that the port is switched to for normal network access. To set the default VLAN globally for all ports on this device, go to model configuration. See [Model configuration on page 338](#) for more information. To set different default VLANs for individual ports, use **Edit Default** on this window.

Network access summary displays the VLAN information for the device. Each port on the device is listed with its current and default VLAN value.

1. Click **Network > Inventory**.
2. Expand the **Container** where the device is located.
3. Right-click the device and select **Network Access/VLANs**.
4. Click **Read VLANs** to get the current and default VLAN values on the device.

Modify current device VLANs

Use this feature to set the VLANs for the device through the FortiNAC UI instead of the command line interface.

1. Click **Network > Inventory**.
2. Expand the **Container** where the device is located.
3. Right-click on the device and select **Network Access/VLANs**.
4. Click **Edit Current** to modify the values on the device.
5. Enter the **VLAN value** for one or more ports.
6. Click **Apply**.

The values are written to the device as the current value.

Modify default device VLANs

Use this feature to modify the default VLANs for the device model in the FortiNAC database.

1. Click **Network > Inventory**.
2. Expand the **Container** where the device is located.
3. Right-click on the device and select **Network Access/VLANs**.
4. Click **Edit Default** to modify the default VLAN values on the device.
5. Enter the **VLAN value** for one or more ports.
6. Click **Apply**.

The values are written to the database model as the default values.

VLAN switching

At times it may be necessary to disable VLAN switching for a specific device until the updated device information is entered/changed in FortiNAC. VLAN usage by the FortiNAC appliance and the device will be out of sync when:

- An administrator discovers/adds a device to the Inventory in the admin UI but does not perform a model configuration to specify the VLANs to be used.
- After the device has already been added to Inventory and configured with specific VLANs, an administrator changes the VLANs on the device itself and does not change the configuration on the FortiNAC appliance to reflect those changes

Disable VLAN switching

VLAN switching is set to enabled by default. FortiNAC uses the default VLAN information for the device when a host connects. To prevent a host from being automatically switched from the new VLAN to the old VLAN during network upgrades, VLAN switching may be disabled. Once the updated information is entered or changed in FortiNAC and the VLAN information has been verified for the device, enable VLAN switching again.

1. Click **Network > Inventory**.
2. Expand the container where the device is located.
3. Click on the device to select it.
4. Right-click on the device and select **Properties**.
5. In the **VLAN Switching** field, select the **Disable** radio button.
6. Click **Apply**, then close the **Properties** window.

Verify the default VLAN

1. Click **Network > Inventory**.
2. Expand the container where the device is located.
3. Click on the device to select it
4. Right-click on the device and select **Network Access/VLANs**.
5. The **Network Access Summary** window is displayed.
6. Verify that the switch/port has the correct default VLAN information.



If the default VLAN has been changed on the switch/ports, the VLAN default settings on the Summary window must be changed as well.

7. Make any changes as needed to the default VLAN settings for each port and click **Apply**.
8. Click **Refresh** on the browser to refresh the view.
9. Verify that the switch/port has the correct default VLAN information.
10. Close the **Summary** window.

Enable VLAN switching

When all the changes to the device have been completed, enable the VLAN switching on the device.

1. Click **Network > Inventory**.
2. Expand the container where the device is located.
3. Click on the device to select it.
4. Right-click on the device and select **Properties**.
5. In the **VLAN Switching** field, select the **Enable** radio button.
6. Click **Apply**, then close the **Properties** window.

Review the model configuration

1. Click **Network > Inventory**.
2. Expand the container where the device is located.
3. Click on the device to select it.

4. Right-click on the device and select the **Device Name > Model Configuration**. This shows the current configuration from within FortiNAC.
5. Compare the VLAN settings to those read from the device. If there is no value for **Default**, hosts get the default specified by the device. In some instances, there may be more than one production default. Also compare the other VLAN settings to the current VLANs read off of the device.
6. Modify the model configuration, as necessary. Set a value for each of the VLANs you want to use. If hosts who are not at risk should get a specific default VLAN, set that value here.
7. Apply your edits and exit model configuration.
8. Select the device, and right-click. Select **Resync Interfaces** to apply the model configuration to the ports on the device.

Poll for contact status

See also [Inventory tree contact status](#).

When Contact Status Polling is enabled, FortiNAC attempts to ping the device at regular intervals. FortiNAC marks the device unreachable if a response is not received within approximately 4 seconds. See table below for retry intervals.

Settings

Field	Description
Contact Status Polling	The number of minutes FortiNAC waits in between polls.

PING Retry Intervals

(Interval settings are not configurable)

PING Request	Wait Interval
1	500ms
2	750ms
3	1125ms
4	1687.5ms

To Poll a device immediately:

1. Click **Network > Inventory**.
2. Expand the container where the device is located.
3. Select the device and select the **Polling** tab.
4. If not enabled, select the **Contact Status Polling** checkbox and click **Save**.
5. Click the **Poll Now** button.

The Last Attempted Poll timestamp will update. If the device responded to the ping requests, the Last Successful Poll timestamp will update to the same value.

Poll for L2 (hosts) information

This option reads the host information on the selected device and updates the Ports tab in Inventory. See [Ports view on page 354](#) for more information. To access this option:

1. Click **Network > Inventory**.
2. Expand the **container** where the device is located.
3. Right-click on the device and select **Polling > L2 (Hosts) Information**.

Ports and hosts

The Ports and Hosts option displays VLAN (Current and Default) and Host (Name and IP) information for each port on the device. If the host name is unknown, the MAC address is displayed.

1. Click **Network > Inventory**.
2. Expand the **container** where the device is located.
3. Right-click on the device and select **Ports and Hosts**.

Device properties

The **Properties** view for devices has Element, System, Polling and Notes tabs. Use these tabs to maintain information about the device and to change settings for the device.

Element view

1. Click **Network > Inventory**.
2. Expand the **container** where the device is located.
3. Right-click on the device and select **Properties**.
4. Click the **Element** tab.
5. Click **OK** to save the changes to this window.

If you have selected a Pingable device instead of a switch or a router, refer to [Add or modify a pingable device on page 302](#) for Settings.

Settings

Field	Definition
Name	Name of the device.
Type	Type of device, such as a switch. May include model information. This information is derived by FortiNAC based on information received from the device.
Physical Address	Only displays for devices that do not have an IP address, such as some wireless access points that are Layer 2 only.

Field	Definition
Has IP address	Only displays for devices that do not have an IP address, such as some wireless access points that are Layer 2 only. If the check box is enabled, then the IP address field can be edited and validated. For devices that do not have an IP address, this box should remain unchecked and no validation will be done when the record is saved.
IP address	IP address of the device.
Vendor / Version	Vendor / Version specific information. This cannot be edited.
VLAN Switching	Enable or Disable. If enabled, FortiNAC automatically switches VLANs using protocols based on the device mapping (SNMP, REST API, etc). If Disabled, VLAN switching is not performed on the device. Note: Disable this option if a customized CLI script is responsible for switching VLANs. See Model configuration.
PA Optimization	If enabled, the Persistent Agent requests the new IP address for its host when the host is moved to a new VLAN. Actions taken by FortiNAC via the switch to request a new IP address for a host, such as blacklisting or shutting down the port, are disabled. Enabling PA Optimization minimizes the amount of time required to renew the host's IP address. This option applies only to hosts with a Persistent Agent. If PA Optimization is disabled, both methods are used to request a new IP address when moving a host to a new VLAN. Hosts with no Persistent Agent are subject to the actions taken by FortiNAC via the switch to supply the host with a new IP address after a VLAN change.
MAC Filtering	Enable or Disable. If enabled, MAC Filtering is performed on the device. For devices which support Secure/Static ports.
Description	Description of the device.
Role	Role for this device. Select a role from the drop-down list.
Incoming Events • Not Applicable • Syslog • Security Events <i>Available when Security Incidents is enabled.</i>	 The availability of this field is dependent upon the type of SNMP device. When Syslog is selected, the following security appliances appear: • FireEye IPS • FortiOS 4.0 • FortiOS 5.0 • PaloAlto Firewall • Sourcefire IPS • TippingPoint SMS • TopLayer IPS When Security Events is selected, the following security appliances appear: • FireEye • FortiOS 4.0 • FortiOS 5.0

Field	Definition
	• PaloAlto • Sourcefire • StoneGate • TippingPoint SMS • TopLayer • Nozomi • Nozomi (2)
Advanced	
Preserve Port Names	Enabled by default. When disabled, any port names/labels that have been changed on the switch will be updated in the FortiNAC database upon the next "Resync Interfaces". To modify at the global level, see Network device. Note: Does not apply to ports on FortiSwitch in either Standalone or FortiLink mode. This is due to a difference in how port names are handled in the FortiSwitch.
Manage as a Generic SNMP Device	Allows FortiNAC to manage an unknown SNMP device where no vendor specific information is available.
Use SNMP To Read L2/L3 Data From The Device	This option displays only for Cisco devices. It allows FortiNAC to read L2 and L3 data and the current VLAN from the device via SNMP instead of the CLI. The check box is not selected by default. However, if you create a device without CLI credentials, the management of the device will default to using SNMP. When using SNMP, full read/write privileges are not required to collect read only L2 and L3 information. However, if you enable SNMP to collect ARP information, duplicate ARP entries cannot be differentiated by time, which results in FortiNAC having outdated IP addresses.
Override Network Device Type	When selected, this option allows you to override the current Network Device Type icon with either a Switch or a Router icon. This does not affect the functionality of the device.
Enable Device Debug	When selected, adds the DEBUG attribute with the value of "TelnetServer ForwardingInterface" to the device. For troubleshooting purposes only. Example of use: 1. Select box and Save. 2. Reproduce behavior. 3. Collect logs for support. See Download Logs. 4. Disable debug. Select box and Save.
Buttons	
Group Membership	View Device Groups. Add the device to a group or remove the device from a group by checking or unchecking the box next to the group name.

System view

1. Click **Network > Inventory**.
2. Expand the container where the device is located.

3. Right-click on the device and select **Properties**.
4. Click the **System** tab.
5. Click **OK** to save the changes to this window.



If the correct Read/Write SNMP credential is specified in the **Element** tab, the name, contact, and location values will be written to the device when you click **Apply**.

The information in the table below is obtained from the SNMP System MIB:

Settings

Field	Definition	MIB Attribute
Name	The name of the device.	sysName
Contact	The contact person for the device	sysContact
Location	The location of the device (for example, Res Hall A, Equipment Closet 1st Floor, Rack 2, Unit 3)	sysLocation
Uptime	The length of time the device has been running	sysUpTime
Description	Description of the device derived by FortiNAC based on information from the device.	sysDescr

Polling view

The Polling tab is where you configure if/when polling will occur, how often, and what will be polled. You can also manually poll the device.

1. Click **Network > Inventory**.
2. Expand the **container** where the device is located.
3. Right-click on the device and select **Properties**.
4. Click the **Polling** tab.
5. Click **OK** to save the changes to this window.

Settings

Field	Definition
Contact Status	
Polling	Enable or disable contact status polling for the selected device.
Poll Interval	Determines how often the device should be polled for communication status. Time is stored in minutes.
Last Successful Poll	Date and time that the device was last polled successfully.
Last Attempted Poll	Date and time that the device was last polled.

Field	Definition
Poll Now	Polls the device immediately for contact status.
L2 (hosts) information	
Polling	Enable or disable polling for hosts connected to the device.
Poll Interval	Determines how often the device should be polled for new host connection information. Time is stored in minutes. Wired device default is 60 minutes. Wireless device default is 10 minutes.
Last Successful Poll	Date and time that the device was last polled successfully.
Last Attempted Poll	Date and time that the device was last polled.
Poll Now	Polls the device immediately for host connections.
L3 (IP-->MAC) information	
Polling	Indicates whether L3 Polling for this device is enabled or disabled.
Poll Interval	Indicates how often the device should be polled for IP information used in IP to MAC address identification.
Priority	Indicates the priority for polling this device. Devices are polled in batches from High priority to Low priority until the required information is found.
Last Successful Poll	Date and time that the device was last polled successfully.
Last Attempted Poll	Date and time that the device was last polled.
Cisco Discovery information	
Global Polling	Indicates whether the global setting for Cisco Discovery Protocol is enabled or disabled. If the global setting is disabled, the feature is disabled for all devices regardless of the setting in the polling field. To change the global setting see Network device on page 910 .
Polling	Indicates whether the Cisco Discovery option for this device is enabled or disabled. Default = Disabled
Poll Interval	Indicates how often the device should be polled for information stored about other connected devices on the network.
Last Successful Poll	Date and time that the device was last polled successfully.
Last Attempted Poll	Date and time that the device was last polled.



If the device you have selected is not capable of L2 polling (polls host connections), L3 polling (polls to do IP to MAC address conversions) or Cisco Discovery, those options are not displayed.

L2 Polling information can also be configured using the L2 Polling window. To access this window select **Network > L2 Polling**. See [L2 polling on page 449](#) for additional information.

L3 Polling information is configured using the L3 Polling window. To access this window select **Network > L3 Polling**. See [L3 polling on page 451](#) for additional information.

Credentials view

Configure or update the credentials to allow FortiNAC to talk to the device. Credentials match the settings on the device.

1. Click **Network > Inventory**.
2. Expand the **container** where the device is located.
3. Right-click on the device and select **Properties**.
4. Click the **Credentials** tab.
5. Click **OK** to save the changes to this window.

The options vary depending on the SNMP protocol selected.

Settings

Field	Description
Validate Credentials	Click to test the CLI and SNMP credentials entered.
SNMP Settings	
SNMP Protocol	Select SNMPv1 or SNMPv3. This option is not available for all types of devices.
SNMPv1	
Security Strings	Click Add to add a security string for the device into the FortiNAC database. This must be the read/write security string. Click Remove. On the window displayed, select and remove security strings for this device from the FortiNAC database. This field displays a list of security strings used during Discovery. The security string most recently used for read/write access is listed first. Also known as the SNMP Community string.
SNMPv3	
User Name	User Name for access to the device. Recommended but not required.
Authentication protocol	
Authentication Password	Enter the password you configured on the device.
Privacy Protocol	Available options are DES and AES-128. Used only for AuthPriv.
Privacy Password	Enter the password you configured on the device. Used only for AuthPriv.
CLI settings	
User Name	The user name used to log on to the device for configuration. This is for CLI access. The user account must have the appropriate permissions configured on the device.
Password	The password required to configure the device. This is for CLI access.
Enable Password	The enable password for the device. This is for CLI access.

Field	Description
Protocol Types	Telnet - Use to log on to the device for configuration. SSH1 - Use to log on to the device for configuration. SSH2 - Use to log on to the device for configuration.
Telnet/SSH Connection Timeout (Sec)	Used to determine how long to wait to connect and/or establish a Telnet/SSH session for this device. When disabled (default), the global setting " Telnet/SSH Connection Timeout (Sec) " applies. See Network device on page 910 This option is also available in the " Set Model Configuration " view. See Virtualized Devices on page 371 and Model configuration on page 338 .
CLI Command Timeout (Sec)	Used to determine how long to wait for a CLI response (prompt, show commands, etc) for this device. When disabled (default), the global setting " Telnet/SSH Connection Timeout (Sec) " applies. See Network device on page 910 . This option is also available in the "Set Model Configuration" view. See Virtualized Devices on page 371 and Model configuration on page 338 .

Modify multiple device properties

You can modify the properties for multiple devices simultaneously. Properties that appear depend on which type of devices are selected.



Settings that are not supported by a selected device will not appear in the view.

Modifications to properties are only applied to selected devices that support those properties. For example, if you select four devices, but only two devices support L3 Polling, a warning icon and tooltip is displayed next to the L3 Polling setting indicating the number of the selected devices that support L3 Polling.

1. Click **Network > Inventory**.
2. Select the **container** where the devices are located.
3. In the **Devices** view, use Ctrl-click or Shift-click to select the devices you wish to modify.
4. Right-click the devices and click **Modify Properties**.
5. Modify the properties for the devices.
6. Click **OK**.

Pingable device properties

The Properties view for Pingable Devices, such as IPS/IDS system, has Element and Details tabs. Maintain device information and change settings on these tabs.

1. Click **Network > Inventory**.
2. Expand the **container** where the device is located.
3. Click on the device and properties are displayed in the right pane.

Element tab settings

Field	Definition
Container	Container in the Topology where this device is stored.
Name	Name of the device
IP address	IP address of the device
Physical Address	The MAC address of the device. Appears in the view only when the device is a pingable.
Device Type	Select the device type from the drop-down list.
Incoming Events - Not Applicable - Syslog - Security Events <i>Available when Security Incidents is configured.</i>	When Syslog is selected, available syslog files appear that can be used by FortiNAC to parse information received from the external devices and generate an event. See Syslog files on page 963. When Security Events is selected, available security event parsers appear that can be used by FortiNAC to parse information received from the external devices and generate a security event. See Security event parsers on page 970.
SSO Agent	- Not Applicable - Custom Script - Palo Alto - RADIUS - iboss
Custom Script	Displayed when Custom Script is selected in the SSO Agent field. Allows you to write and select a script that will integrate with a SSO Agent that is not currently supported.
Apply to Group	Select this check box to apply the Custom Script SSO options only to the selected Host group in the drop-down list. If you do not select the check box, the SSO options are applied to all Host groups.
RADIUS Accounting Port	Displayed when RADIUS is selected in the SSO Agent field. Port on the Fortinet Single Sign-On User Agent configured to receive RADIUS Accounting messages from external devices. This port must match the port configured in Fortinet.
RADIUS Secret	Displayed when RADIUS is selected in the SSO Agent field. Must match the RADIUS secret configured for FortiNAC in Fortinet.
Apply to Group	Select this check box to apply the RADIUS SSO options only to the selected Host group in the drop-down list. If you do not select the check box, the SSO options are applied to all Host groups.
XML API Port	Displayed when Palo Alto User Agent is selected in the SSO Agent field. Port on the Palo Alto User Agent configured to receive messages from external devices. This port must match the XML API port configured on the Palo Alto User Agent. See Add or modify the Palo Alto User-ID agent as a pingable on page 304.
Domain Name	Displayed when Palo Alto User Agent is selected in the SSO Agent field. FQDN for your network users' domain. This is sent with the logged in user ID to Palo Alto.

Field	Definition
Use Integrated Agent	When selected, FortiNAC will integrate with the firewall directly.
API Key	Displayed when the Use Integrated Agent check box is selected. Enter the API Key value. The key can be retrieved manually or by selecting Retrieve .
Apply to Group	Select this check box to apply the Palo Alto SSO options only to the selected Host group in the drop-down list. If you do not select the check box, the SSO options are applied to all Host groups.
iboss Port	Displayed when iboss is selected in the SSO Agent field. The IBOSS port is the IBOSS HTTP port that is used to talk to the IBOSS SSO agent. The IBOSS port is defined in the IBOSS SSO GUI.
iboss Key	Displayed when iboss is selected in the SSO Agent field. The IBOSS key is a security key used to talk to the IBOSS SSO agent. The IBOSS key is defined in the IBOSS SSO GUI.
iboss Domain	Displayed when iboss is selected in the SSO Agent field. The iboss Domain is a required field that allows the user to enter their Active Directory Domain Name.
Apply to Group	Select this check box to apply the iboss SSO options only to the selected Host group in the drop-down list. If you do not select the check box, the SSO options are applied to all Host groups.
Role	The Role for this device. Available roles appear in the drop-down list.
Description	Description of the device entered by the Administrator.
Note	User specified notes about the device.
Contact Status Polling	Enable or disable contact status polling for the selected device.
Poll Interval	Determines how often the device should be polled for communication status. Time is stored in minutes.
Poll Now	Polls the device immediately for contact status.
Last Successful Poll	Date and time that the device was last polled successfully.
Last Attempted Poll	Date and time that the device was last polled.

Details tab settings

Field	Definition
Host Name	Name of the device.
Department	Name of the department.
Owner	Name of the owner of the device.
Administrative Contact	Administrative contact person for the device.
Geographical Location	Geographical location of the device (for example, Res Hall A, Equipment Closet 1st Floor, Rack 2, Unit 3).

Field	Definition
Business Purpose	Business purpose of the device.
BOOTP Address	IP address for the BOOTP Protocol.
Print Queue	Name of the print queue for the device.

View role membership

View a list of the role(s) assigned to the selected device or port and the network access ID for that role on the device.

1. Click **Network > Inventory**.
2. Expand the container where the device is located.
3. Click on the device to select it and display associated ports in the right pane.
4. **To view roles for the device:** Right-click on the device and select **Role Membership**.
5. **To view roles for a port:** Right-click on a device port in the right pane and select **Role Membership**.

Settings

Field	Definition
Role	Name of the role.
CLI	Allows you to apply a CLI configuration to a device or port when this role is used.
Access Value	The Access ID (VLAN ID, VLAN Name, or Role) information associated with this role on the device or port.
Locations	The location defined for the Network Device Role.

Set device mapping for unknown SNMP devices

If an SNMP Device is added to the Topology, but the device could not be identified by the OID, the option will be available to set the device mapping.

1. Select **Network > Inventory**.
2. **Right-click** on the device marked with a question mark icon.
3. Select the **Set Device Mapping** option from the menu.

Settings

Field	Definition
Delete Existing Mapping	Removes the custom mapping currently set for that model. Once the mapping is removed, the device icon will revert to a "?" until another mapping is set or device support is added for the device's system OID. Note: This button will not display in models that are using system defined mappings.
Name	Name of the selected device.

Field	Definition
OID	Detected OID of the selected device.
Description	Description of the device read via SNMP or supplied within the Element details.
Standard Bridge MIB	Whether or not the device appears to support the standard Bridge MIB, 1.3.6.1.2.1.17.
Standard VLAN MIB	Whether or not the device appears to support the standard Switch VLAN MIB, 1.3.6.1.4.1.207.8.9.2.5.2.
Standard IP MIB	Whether or not the device appears to support the standard IP MIB, .1.3.6.1.2.1.4.28.
Current Mapping	The source used for the current Device Mapping for the selected device. If modeled as an existing device mapping, this will list the OID of the device it cloned.
Report Mapping Details to Fortinet	If checked, the details of this mapping will be e-mailed using the configured mailer to Fortinet, so we may add them to our product. The e-mail sends only the following information: • Logged On User • Logged On User Email • Appliance Physical Address • Device OID • Device Description • Chosen OID
Model this Device as a Generic SNMP Device	The device will be managed using the available SNMP MIBs. It may require additional details in the Model Configuration to specify VLANs.
Model this Device as a Device Type	The device is not manageable using standard SNMP MIBs. It may be modeled as an SNMP enabled network device of the type specified in the drop-down.
Model this OID from an Existing Device	All devices with the same OID will be mapped when this is selected, if they have not already been mapped as a Generic SNMP Device or Device Type. This OID will have all properties copied from an existing Device Model. Double click a Device Model to see more information.
Device Model	The name of the Device Model copied to this OID. Typing in this field will search the Device Mappings table based on both OID and Model.

Update device mapping

When new devices are added to the FortiNAC Inventory, recognized device types are displayed with an icon indicating the type of device. The system name (sysName) is used for the name of the device. If the device type is not recognized, a question mark icon is displayed and more information is required to manage the device.

Unrecognized devices which support the IETF standard MIBs listed below can be added as generic SNMP devices. This “Generic SNMP” feature allows hosts to be read, VLANs to be read/switched and IP to MAC address information to be read from the device – without needing a specialized code patch or build. In order to successfully configure a Generic SNMP device, it must fully support the MIB groups as described in the following table.



Devices that appear to support the standard VLAN MIB, may not fully support the standards. The switching of a VLAN on a port may or may not be supported by the device.

Standard	Reference	SNMP MIB Objects/Tasks
RFC1213 – MIB II	Address Translation (AT) MIB	Read of IP->MAC: atTable - The Address Translation tables contain the NetworkAddress to 'physical' address equivalences. SNMP OIDs 1.3.6.1.2.1.3.1.1.2
RFC1158 - MIB II	Address Translation (AT) MIB	Read of IP -> MAC: atTable - The Address Translation Group contains NetworkAddress to 'physical' address equivalences - deprecated by MIB II. ipNetToMediaTable - The Address Translation tables contain the NetworkAddress to 'physical' address equivalences. SNMP OIDs 1.3.6.1.2.1.3.1.1.2 1.3.6.1.2.1.4.22.1.2
RFC1493 – BRIDGE-MIB	BRIDGE MIB	Read Hosts: dot1dTpFdbTable - A table that contains information about unicast entries for which the bridge has forwarding and/or filtering information. SNMP OIDs 1.3.6.1.2.1.17.4.3.1.1 1.3.6.1.2.1.17.4.3.1.2 1.3.6.1.2.1.17.4.3.1.3
RFC2674-Q-BRIDGE-MIB	VLAN MIB	Read / Switch VLANS: dot1qPortVlanTable - A table containing per port control and status information for VLAN configuration in the device. SNMP OIDs 1.3.6.1.2.1.17.7.1.4.5.1.1



Do not change an existing supported device to a generic SNMP device or you will lose the custom options provided in FortiNAC for that device.



If support for a generic SNMP device is added in a later release of FortiNAC, you can either leave the device as generic SNMP device or delete it and re-add it to the Inventory. Deleting the device removes it from all device and port groups. The device and its ports would have to be added to the appropriate groups again manually.

Update unknown SNMP devices

The existence or absence of the SNMP MIB objects determines the type of device to add. Based on the combination of SNMP MIB objects found, options on the Update Image dialog are dynamically adjusted.



If you try to update a device that is no longer in contact with FortiNAC, you will see the following message. “This Device indicates that - Contact is not established with this device.” When that message is displayed you only have the option to select a device type. Update Device Mapping will not be able to determine whether the device is a switch or a router.

1. Select **Network > Inventory**.
2. **Right-click** on the device marked with a question mark icon.
3. Select the **Update Device Mapping** option from the menu.
4. See the examples listed below for additional information.

Example 1

The following example shows the options for a device that supports both the standard BRIDGE MIB, the standard VLAN MIB and the standard IP MIBs. Therefore, it is likely that this device is a switch. However, if you know this device is not a switch, click the **Model this Device as** option and select the appropriate device type from the drop-down list.

After updating the image in the Inventory, go to Model Configuration to specify VLANs. See [Model configuration on page 338](#) for additional information.

When testing the device for VLAN switching, check the Events View for a VLAN Switch Failure event. If a VLAN Switch Failure is generated for this device, then the device does not support the standard VLAN MIB. You will not be able to switch VLANs.

Example 2

The following example shows a device that supports the standard IP MIBs, but does not support the BRIDGE MIB. Therefore, it is likely that this device is a router. However, if you know this device is not a router, click the **Model this Device as** option and select the appropriate device type from the drop-down list.

Example 3

The following example shows a SNMP device that does not support the standards. This indicates that the device is neither a switch nor a router. In this example, the device is an alarm system and you can map it as an alarm system with the appropriate icon. You can leave it as an SNMP device and use the **Model this Device as** option to select the type. When selected the device will display the SNMP interfaces in the panel on the right pane of the Inventory.

If you prefer to see device information instead of the interfaces, go to the Host View, right-click on the device and select Register as Device.

Another option is to delete the device from the Inventory. Right click on the container and use the Add Pingable option from the menu to add the device.

Firewall session polling

Use firewall session polling to request information about your network from FortiGate devices. FortiNAC can use information learned from polling to identify devices. For more information, see [Profiled devices on page 251](#).

To configure firewall session polling:

1. Go to **Network > Inventory**.
2. Expand the container where the device is located.
3. Right-click the device and click **Set Firewall Session Polling**. This option is only available for FortiGate devices.
4. Select **Enabled**.
5. Enter the polling **Frequency** (the default is five minutes).
6. (Optional) Select **Create Rogues from Session Data**.
7. (Optional) Click **Poll Now** to receive polling information from the device immediately.
8. Click **OK**.

To view the polling information, go to **Users & Hosts > Network Sessions**. For more information, see [Network sessions on page 274](#).

NOTE: It is possible not all sessions displayed in the FortiGate UI will be displayed in FortiNAC. FortiNAC displays network sessions based on REST API: `api/v2/monitor/firewall/session/select`

There are different sessions shown in the FortiGate UI which are not present in this API response. FortiNAC does not display these sessions. For details see article [386368](#).

Modifying Switch Components in a Stack

Typically, a device's interfaces remain fairly stable and unchanging. However, devices that reside in a chassis or those that can be stacked share management between separate boards or stacked units. When boards or units are added, removed, or repositioned within the chassis or stack, it is necessary to have FortiNAC re-read the device to learn of the changes and display an accurate representation in the Ports tab in Inventory. See Resync interfaces.

Note: If the indexing has changed and FortiNAC needs to remodel the interfaces, FortiNAC will delete and recreate new port models to represent the re-indexed switch interfaces. This will affect manual port grouping done for the interface models.

Device configuration

To successfully monitor and configure certain vendor devices, you must set some additional configuration parameters. Access these parameters through the **Model Configuration** view and set them prior to scheduling actions on the device.

1. Click **Network > Inventory**.
2. Expand the container where the device is located.
3. Right-click on the device and select one of the options in the table.

Option	Description
Device Name > Global Model Configuration	Configure global database model parameters for all devices of this type across the network.
Device Name > Model Configuration	Configure database model parameters for the selected device.
Device Name > Running Configuration	View the configuration running on the selected device (device dependant). This option is only available for some devices.
Device Name > Static/ Secure Port Configuration	Configure static or secure ports on the selected device (device dependent).

Delete a device

1. Click **Network > Inventory**.
2. The Network Devices window displays.
3. Select a device from the list in the Network Devices panel.
4. Click **Delete**.
5. The program asks if you are sure. Click **Yes** to continue.

Resync Interfaces

It is necessary to have an accurate representation of a device's interfaces in the Ports tab in Inventory. This option reads the interface information from a modeled device and updates FortiNAC's representation of that device.

The information in the port name (listed under the "Name" column in Port View) is built using switch name, ifName and ifDescription. Ports or interfaces are displayed in the order in which they appear in the interface table on the device. Depending on the device and its configuration, ports may not display in order numerically or alphabetically.

Resync Interfaces only updates the interface status under normal conditions. To enable FortiNAC to update the description as well as port status when Resync Interfaces is run, see "Enable Port Description Overwrite" below for instructions.

Devices that reside in a chassis or those that can be stacked share management between separate boards or stacked units. When boards or units are added, removed, or repositioned within the chassis or stack, it is necessary to have FortiNAC re-read the device to learn of the changes and display an accurate representation. If the port sequence has changed, Resync Interfaces will update index, status and port name.

Example: Chassis modeled in FortiNAC with boards in slots 1, 3 and 4

- FortiNAC will re-index if a board is inserted in slot 2
- FortiNAC will not re-index if a board is inserted in slot 5

If re-indexing is necessary, FortiNAC deletes and recreates new interface models to represent the re-indexed switch interfaces.

Note: When interface models are deleted and recreated, the manual port grouping done for those interface models is affected. It is recommended to review port groups if a new module has been inserted and Resync Interfaces run.

To access this option:

1. Click **Network > Inventory**.
2. Right-click on the device and select **Resync Interfaces**.
3. Click **Yes** on the confirmation dialog to continue.

Enable Port Description Overwrite

Port descriptions in Inventory are updated if the port descriptions on the actual switch have changed. Updates occur when one of the following is done:

- FortiNAC services are restarted.
- Resync Interfaces is run on the device model (either manually or through a scheduled task) when "Preserve Port Names" is disabled. See [Device Properties](#).

Model configuration

The model configuration window allows you to configure devices that are connected to your network so that they can be monitored. Data entered in this window is stored in the FortiNAC database and is used to allow interaction with the device. Passwords are encrypted. Data entered on the model configuration window is not sent to the device. This window can be accessed from the Topology and from the Network Devices window.

Models Using a Virtual IP (VIP) Address: SSH communication can fail if the device controlling the VIP changes. This is due to a change in the SSH key, making the currently used key invalid. To prevent an SSH communication failure due to this scenario, the MultiKnownHostEntries attribute can be enabled in FortiNAC CLI. For details and instructions, see [Configure SSH Keys for VIP](#).

When configuring the device itself, use only letters, numbers and hyphens (-) in names for items within the device configuration, in security strings and in SNMP credentials. Other characters may prevent FortiNAC from reading the device configuration. For example, in many cases the # sign is interpreted by FortiNAC as a prompt. Cisco restricts the use of @ and #.



For network devices using API credentials, the User Name is the serial number of the appliance and the Password is the REST API Key.

Access from Topology

1. Click **Network > Inventory**.
2. Expand the Container icon.
3. Right-click on the device, and then click **Model Configuration**.

Settings

Device configuration information is specific for each device and may include any combination of the fields in the table below:

Settings	Description
General	
User Name	The user name used to log on to the device for configuration. This is for CLI access.

Settings	Description
	 The user account must have the appropriate permissions configured on the device.
	For network devices using API credentials, the User Name is the serial number of the appliance.
Password	The password required to configure the device. This is for CLI access. For network devices using API credentials, the Password is the REST API Key.
Enable Password	The enable password for the device. This is for CLI access. Note: Version 8.7.2 and higher: Arista switches can be configured to require typing "enable" to enter enable mode, but no password is needed. For such configurations, populate this field with the # character.
Super Password	The super password required for access to more features on 3Com devices.
HWC Connect Port	Port for the External Captive Portal that was configured by the user on the device during the initial device setup. This port is required for FortiNAC to send commands to the device. Consult the manufacturer for assistance in locating this port number.
Read Groups From Device	Ports on a device can be placed in to network groups that control access. This option reads the preset groups from the device.
Enable RADIUS authentication for this device	When selected, FortiNAC will process RADIUS requests from the device.
Clear Known Hosts	Clear all known host keys associated with this device. Host keys for devices modeled in Inventory are written to /bsc/.ssh/known_hosts.
Telnet/SSH Connection Timeout (Sec)	Used to determine how long to wait to connect and/or establish a Telnet/SSH session for this device. When disabled (default), the global setting " Telnet/SSH Connection Timeout (Sec) " applies. See Network device .
CLI Command Timeout (Sec)	Used to determine how long to wait for a CLI response (prompt, show commands, etc) for this device. When disabled (default), the global setting " Telnet/SSH Connection Timeout (Sec) " applies. See Network device .
Protocol types	
Telnet	Use Telnet to log on to the device for configuration.
SSH1	Use SSH1 to log on to the device for configuration.
SSH2	Use SSH2 to log on to the device for configuration.
VLAN ID/Network Access	
VLAN Display Format	For some devices, the list of VLANs configured on the device can be read from the device and made available in a drop-down. When this feature is available, the VLAN Display Format option is shown. Choices included:

Settings	Description
	• VLAN Name: Displays a drop-down list of VLANs configured on the device by VLAN name for each isolation state. • VLAN ID: Displays a drop-down list of possible VLANs configured on the device by VLAN ID or number for each isolation state. • Manual: Provides an empty text field to enter the VLAN name or ID. This is used in the event that the VLANs on the device have not been pre-configured
Read VLANs	Read VLAN configuration from the device and populate the drop-down lists of VLANs for each isolation state.
Default	The Default VLAN value is stored in the FortiNAC database and is used when the VLAN is not determined by another method, such as a network access policy. Typically, if a VLAN is specified as the Default, it is the VLAN used for "normal" or "production" network access. It will be used for all the untagged (non-uplink) ports on the device. If you do not want all ports on the device to use the same "Default" VLAN, you can leave the value blank in Model Configuration and use Network Access/VLANs to customize the default VLANs for each port. See Network access/VLANs on page 319 for more information.
Dead End	The dead end VLAN for this device. Isolates disabled hosts with limited or no network connectivity from the production network.
Registration	The registration VLAN for this device. Isolates unregistered hosts from the production network during host registration.
Quarantine	The quarantine VLAN for this device. Isolates hosts from the production network who pose a security risk because they failed a policy scan.
Authentication	The authentication VLAN for this device. Isolates registered hosts from the Production network during user authentication.
Voice	The voice VLAN (s) for this device. This field accepts a list of VLANs separated by commas, such as 10, 25,30. This indicates to FortiNAC that these VLANs are excluded from all other uses.
Apply Default VLAN ID To All Non-wireless ports	If a device has both wired and wireless ports, you may choose to assign VLANs to each port individually. You may also choose to assign a single default VLAN to all of the wireless ports for this device, by putting a VLAN ID in the Default field on this window. That number then overrides the individual entries on the wireless ports. The wired ports would continue to have a separate VLAN setting for each port. If you choose to apply the Default VLAN ID to both wireless and wired ports, enabling this feature overrides the original port settings on the wired ports with the setting in the Default field on this window
Manage Captive Portal	Affects only Meru Controllers. If the Captive Portal setting on any Security Profile for any SSID is set to WebAuth indicating that the SSID is being managed by Internal Captive Portal (ICP) on the Meru Controller and this check box is enabled, all SSIDs set to WebAuth will be managed by FortiNAC.

Settings	Description
	If enabled, FortiNAC uses Firewall Rules to treat authenticated and unauthenticated users differently. The treatment selected in the Access Enforcement section of model configuration is ignored for any SSIDs set to WebAuth. Hosts that are isolated are treated as unauthenticated hosts regardless of the isolation type. Hosts that are not isolated are treated as authenticated.
VLAN Management	Introduced in FortiNAC version F 7.6.3. Option available for select HP 1900 switches only. Tagged Only (default): Switches the ports VLAN and modifies the Egress Ports for both the old & new VLAN. UntaggedOnly: Switches the ports VLAN and modifies the Untagged Ports for both the old & new VLAN. All: Switches the ports VLAN and modifies the Egress & Untagged Ports for both the old & new VLAN.
CLI configurations	
Configurations	This section allows you to associate pre-configured scripts with selected Port states or host states. A default script can also be selected. Scripts are not required. States that can be associated with CLI configurations include: default, registration, authentication, dead end, and quarantine. See CLI configuration on page 433 for information on creating scripts. Note: Disable the VLAN Switching option in the Elements tab if a customized CLI script is responsible for switching VLANs. See Device properties.
RADIUS	
Primary RADIUS Server	The RADIUS server used for authenticating users connecting to the network through this device. Select the Use Default option from the drop-down list to use the server indicated in parentheses. See RADIUS on page 375 for information on configuring your RADIUS servers.
Secondary RADIUS Server	If the primary RADIUS server fails to respond, this RADIUS server is used for authenticating users connecting to the network until the primary RADIUS server responds. Select the Use Default option from the drop-down list to use the server indicated in parentheses.
RADIUS Secret	The secret used for RADIUS authentication.  The RADIUS secret used must be exactly the same on the wireless device, on the RADIUS server and in the FortiNAC software under RADIUS Settings and Model Configuration.
Modify Button	Allows you to modify the RADIUS secret.
Mode	The RADIUS Authentication Mode to be used when a RADIUS request is received from the modeled device.

Settings	Description
	Local: Use the Local RADIUS server. Enter the RADIUS Secret, and choose the attributes to be sent in the Accept packet. Proxy: Use the RADIUS Proxy. Optionally choose to override the RADIUS server to proxy to and enter the RADIUS secret.
Default RADIUS Attribute Group (Local RADIUS Option)	The default RADIUS Attributes to be sent for all accepted requests from this device. Hover over the group name to see what attributes and values will be sent. FortiNAC has pre-built attribute groups that can be used for most devices.
RFC5176 settings	 See the RFC5176 CoA/Disconnect Message Cookbook for more details. RFC5176 Mode The RADIUS RFC5176 Mode to be used for dynamic authorization change, for example, an authenticated host switches VLAN. • System defined: Use the system defined RFC5176 settings (Disconnect message with default attributes) • Custom: Use custom RFC5176 settings. Port, message type and attribute group can be configured in sections below. • Multiple connection: Force the system to use the RFC5176 Message type and Attribute Groups under RFC5176 to build up the CoA/Disconnect message if certain conditions are satisfied. • Daisy chain: Configure FortiNAC to send unique attributes to the port if the hosts are daisy-chained. RFC5176 Port The port that receives CoA and Disconnect messages. By default, it is 3799. Note: this feature only shows when Custom is selected. RFC5176 message type Choose the type of message that will be sent during dynamic authentication change: CoA or disconnect message. Note: this feature only shows when Custom is selected. RFC5176 attribute group Attributes that will be sent during dynamic authentication change.
Restricted access	
Object Group Name	Network List name that is used to contain IPs when the host is marked safe.
Network access - wireless devices	

Settings	Description
SSO Addresses	Network Address group containing the desired scope of IP's to be managed using SSO. In FortiGate integrations, this field can be used for both FSSO and Dynamic Address tags. See Addresses. Important: Requires a resync to apply changes. For instructions, see Resync Interfaces.
VPN Addresses	Network Address group containing the desired scope of IP's to be managed over VPN. See Addresses. Important: Requires a resync to apply changes. For instructions, see Resync Interfaces.
Source IP Address	Device's IP address used for communication. Required if this address does not match the IP address in the Element tab.
Read Roles From Device	Retrieves roles that currently exist on the device being configured.
Read Roles	The drop-down next to each type, such as Registration, contains a list of possible roles read from the device. You can select a role for one or more of the types listed below. • Default • Dead End • Registration • Quarantine • Authentication
Host State	Host State is used to determine treatment when the host connects to the network. For each host state select an option in the Access Enforcement column and where applicable in the Access Value column. • Default • Dead End • Registration • Quarantine • Authentication • Roaming Guest  Roaming Guest is a special host state detected when a user authenticates using a domain name that is not listed in the local domains list. Users are authenticated via a remote RADIUS server and are placed on the network immediately unless Deny is selected under Access Enforcement. Roaming guests bypass the captive portal and device profiler. See Roaming guests on page 901.
Access Enforcement	This set of drop-down menus works in conjunction with the Host States listed above to determine treatment for hosts when no VLAN/Role value is supplied or when access control is being enforced. Options include: • Deny: Host will be denied access to the network when it is in this state. For example, if the host is not registered and Registration is set to Deny, the host connection will be rejected.

Settings	Description
	 Endpoints that have been denied access may continuously request access which can unnecessarily consume system resources. • Bypass: Host will be allowed access to the network when it is in this state. The host will be placed on the default VLAN/Role configured on the device for this port or SSID. For example, if Quarantine is set to Bypass, hosts that fail a scan and would normally be placed in Quarantine are placed in the default VLAN/Role on the device. • Enforce: Indicates that the host will be placed in the VLAN/Role specified in the Access Value column for this state.
Access Value	VLAN/Role where a host in this state should be placed when it connects to the network. If Enforce is selected in the Access Enforcement field you must enter a value in the Access Value field.
Additional RADIUS Attribute Group (Local RADIUS option)	For each Logical Network, you can choose to either use the default values only, or to append and overwrite with another attribute group. Hover over the group name to see what attributes and values will be sent.
RFC5176 Message Type	Can use default (none) or overwrite with custom settings. Choose the type of message that will be sent during dynamic authentication change: CoA or disconnect message. Note: Settings for a logical network work only if a device is switching to this network.
RFC5176 Attribute Group	The attributes that will be sent during dynamic authentication change. The user can use default (none) or overwrite with custom settings. Attribute Group is required when the message type is not marked as "none." For Default Logical Network > edit page in SSID or Virtualized Devices, there is no RFC5176 fields for the user to fill in; FortiNAC will use the settings in Device Level. Note: Settings for a logical network work only if a device is switching to this network.
Wireless AP parameters	
Preferred Container Name	If this device is connected to any Wireless Access Points, they are included in the Topology. Enter the name of the Container in which these Wireless Access Points should be stored. Containers or folders are created in the Topology to group devices.
Detail configuration	
Check box	Secure Ports is enabled for ports on this device. When this option is enabled, secure ports allows you to deny access to disabled hosts. See Secure port/static port overview on page 349 for requirements.

Global model configuration

FortiNAC maintains a model of each device it manages in the database. Those database models of physical devices contain information about how to communicate with the device, what VLANs should be used for isolation, which RADIUS server should be used for authentication and what the communication protocol is.

Device-specific information varies by vendor. You can set and store some configuration parameters globally across a specific vendor's devices by using FortiNAC's Global Model Configuration option. This window can be accessed from the Inventory and from network devices.

When configuring the device itself, use only letters, numbers and hyphens (-) in names for items within the device configuration, in security strings and in SNMP credentials. Other characters may prevent FortiNAC from reading the device configuration. For example, in many cases the # sign is interpreted by FortiNAC as a prompt. Cisco restricts the use of @ and #.

Access from Inventory

1. Click **Network > Inventory**.
2. Expand the **Container** icon.
3. Right-click on a device manufactured by the vendor of the group of devices to be configured, select the device name, and then click **Global Model Configuration**.

Configuration

1. On the **Global Model Configuration** window use **Ctrl-Click** to select one or more devices from the list in the **Select Devices** section.
2. Select one of the Save options:
 - **Save all values for selected device models** saves all data that is displayed on the configuration window to the models in the database for all devices that have been selected. For example, if you have created a model in the database for one device and would like to create the same model for several others, you could go to Network Devices, right-click on the "copy from" device and select Global Model Configuration. The values for the selected device are displayed. Then, select additional devices for which you want to create models. Click the Save All values option and all of the device models will be saved with the same information as the first one.
 - **Save only changed values for selected device models** saves only those fields that have been modified to the models in the database for all devices that have been selected. For example, if you have set the user names and passwords on several of your switches to be the same, those modifications must be entered in the model configuration stored in the database to allow FortiNAC to communicate with the devices. Updating the user names and passwords can be done all at once by selecting multiple devices of the same brand, entering the new user name and password and choosing the Save only changed values.
3. The information entered in the configuration is model-specific. See [Model configuration on page 338](#) for information on each field that you can configure.
4. Click **Apply**.

If you have chosen to Save all values, every field is copied exactly as it displays to the model configuration record of each of the selected devices, including blank fields. A warning is displayed.

If you have chosen to Save only changed values, only the fields highlighted in orange will be saved to the model configuration record of each of the selected devices. A warning is displayed.

Configure SSH Keys for VIP

SSH communication can fail if the device controlling the VIP changes. This is due to a change in the SSH key, making the currently used key invalid. To prevent an SSH communication failure due to this scenario, the MultiKnownHostEntries attribute can be enabled in FortiNAC CLI. FortiNAC's known_hosts cache is checked for all potential matches of the VIP and determine which entry to use. This is done on a per-device model basis.

1. Log in to the FortiNAC CLI as admin.
2. Add the IP address of a device that could potentially own the VIP to the known hosts cache. Type:

```
execute ssh-known-hosts add current-user <username> <IP address>
```


When prompted to continue connecting type **yes**.
3. Type **Ctrl-C** to end the SSH session.
4. Copy the key and associate the IP address to the VIP.

```
execute ssh-known-hosts duplicate current-user <IP address from step 2> <VIP>
```
5. Confirm the change by entering the following command:

```
execute ssh-known-hosts show current-user | grep <VIP address>
```
6. Two entries for the VIP should return with 2 different keys:
1 entry is the VIP which is modeled in FortiNAC as a full device model SSH key
1 entry is the pingable model
7. Repeat steps 2-4 for each device that could potentially own the VIP
8. Enable the MultiKnownHostEntries attribute for the VIP. Type:

```
execute enter-shell  
device -ip <VIP address> -setAttr -name MultiKnownHostEntries -value true
```


Example:

```
execute enter-shell  
device -ip 10.20.20.3 -setAttr -name MultiKnownHostEntries -value true
```

Set CDP polling

You use Cisco Discovery Protocol (CDP) polling to allow FortiNAC to gather information about network devices more quickly and efficiently. Network devices that are configured for CDP collect and store information about the network devices they manage or can contact. Devices that have the capacity for CDP must have the feature configured on the device's firmware.

CDP polling is enabled by default.

1. Go to **System > Settings > Network Device**.
2. Select **Enable Cisco Discover Polling**.
3. If required, select **Maximum Cisco Discovery Depth** set a limit for the number of layers from the FortiNAC that are queried.
4. Select **Save Settings**.

Wired devices and 802.1X

802.1X authentication, which provides FortiNAC with another means of port-level access control, is currently supported for a number of devices including:

- Ubiquiti
- Nokia
- Meraki
- Aerohive wired
- Alcatel/Lucent
- Apresia

-
- Foundry/Brocade/Ruckus
 - Cisco
 - Fortinet/Fortigate
 - HP/Aruba ProCurve
 - Juniper
 - Nortel/Avaya/Extreme

Support for additional devices will be provided based on the number of customer requests and the availability of similar equipment.

Host configuration

Host supplicants should be configured to authenticate using user credentials, not host information, such as hostname. This will give FortiNAC the user information to associate with the host/device allowing for automatic authentication.

HP switches must have a time-window of 0 for the most consistent results.

FortiNAC configuration

- In FortiNAC set up one or more RADIUS servers for authentication. See [RADIUS on page 375](#) for additional information.
- Make sure that the RADIUS secret is the same everywhere, including: the RADIUS server itself, RADIUS server settings configured in FortiNAC, RADIUS settings configured on model configuration and in the configuration for your device. If the RADIUS secret does not match in all locations, authentication requests will fail.
- Add the Device to FortiNAC using the Discovery process or by adding the device manually. See [Discovery on page 311](#) or [Add or modify a device on page 299](#).
- After the device is added to FortiNAC you must complete the model for the network device in the database. See [Model configuration on page 338](#).
- If VLAN switching is not enabled, no VLAN will be assigned to an authentication response. Verify that VLAN Switching is enabled under Device Properties.
- Ports on the device that will manage connected hosts should be placed in the appropriate access control groups, such as: forced registration, forced authentication, or forced remediation. If ports are not added to these groups, the isolation VLANs associated with those states will not be provided in an authentication response for those ports. See [Groups on page 843](#).

Device configuration

Define the FortiNAC Server as the RADIUS server for the devices you want to manage with FortiNAC as follows:

- Use the management IP address of your FortiNAC Server as the IP of the RADIUS server.
- If you are setting up FortiNAC as the RADIUS server for a device in a high availability environment, you must use the actual IP address of the primary control server, not the Shared IP address. Set up the secondary control server as a secondary RADIUS server using its actual IP address. Regardless of the environment, you may also want to set up your actual RADIUS server to be used in the event that none of your FortiNAC appliances can be reached. This would allow users to access the network, but they would not be controlled by FortiNAC.

Cisco device configuration

Cisco switches include numerous features with their 802.1x support, many of which are not affected by this integration. Administrators should be familiar with configuring 802.1x port-based authentication on the relevant switches. Many options can be configured that affect the authentication behavior on the device, such as host mode (ie. single-host and multi-host modes) and IP phone support. It is recommended that you have a thorough understanding of these features before deploying 802.1x.

Cisco features that are affected by the integration with FortiNAC include the following:

- Configuring VLANs for the guest, auth and critical values is not supported. FortiNAC does not currently detect how a port has been assigned a VLAN. FortiNAC always assumes it is in control over the VLAN to which a port is assigned. Therefore, if these VLANs are configured, FortiNAC may still attempt to affect a VLAN change on the port based on the connected host state.
- Ensure that RADIUS requests sent by the Cisco router contain the Cisco-NAS-Port vendor specific attribute. FortiNAC uses this attribute to identify the port involved in the authentication.
- MAC-authentication bypass is supported, but administrators should be careful to set a reasonable delay. The switch waits for the delay period for the EAPOL message prior to using MAC-authentication. Connecting hosts will be delayed by at least that amount when no supplicant is present or enabled.

IOS configuration statements relating to 802.1x

The statements listed below represent a minimal configuration to enable 802.1x on a Cisco switch/router running IOS. The commands may vary based on switch model and IOS version. These are taken from a Cisco 3750 -24TS running IOS 12.2(25)SEE3.

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa nas port extended
```

(required to enable Cisco-NAS-Port)

```
!
interface FastEthernet1/0/18
switchport access vlan 163
```

(Port will only be assigned this VLAN if none is assigned or exception condition occurs.)

```
switchport trunk encapsulation dot1q
switchport mode access
dot1x mac-auth-bypass (optional)
dot1x pae authenticator
dot1x port-control auto
dot1x host-mode multi-host
dot1x timeout quiet-period 3
dot1x timeout server-timeout 10
dot1x timeout reauth-period 180
dot1x timeout tx-period 5
dot1x timeout supp-timeout 6
dot1x reauthentication
!
radius-server host 192.168.34.31 auth-port 1812 acct-port 1813 key abc123
radius-server source-ports 1645-1646
radius-server vsa send authentication
```

Secure port/static port overview

When multiple hosts connect to the same port on a device or you do not have a Dead End VLAN it can be difficult to disable individual hosts. Filtering for a particular physical or MAC address is one option for disabling a host. Options vary depending on the capabilities of the device to which these hosts are connected.

If the device supports either secure ports or static ports, you can designate a secure/static port which becomes the equivalent of a Dead End VLAN. When a host is disabled either manually or by an alarm action, a message is sent to the device indicating that this MAC address has been disabled. The MAC address is placed in a list on the device which indicates it only has permission to use the port designated as secure or static. If the host connects on any other port, it cannot access anything.

Make sure that the port designated as static or secure is not accessible. If a disabled host were to connect to that port, it would have network access.

To use this feature you must configure the following:

FortiNAC

- In the Model Configuration for the device you must enable secure ports. See [Model configuration on page 338](#) for instructions and Settings.
- When secure ports has been enabled, you must designate a port on the device as the secure or static port.
- This device must belong to the Physical Address Filtering group. This group is a default system group and should already exist. See [Modify a group on page 846](#) for instructions on adding the device to the group.
- Membership in the Physical Address Filtering group may cause VLAN switching to occur. See [Modify a group on page 846](#).

Device

The device itself may or may not require any additional configuration.

- **Alcatel:** Alcatel switches do not require any special configuration in order to support Physical Address Filtering.
- **3Com, Cisco, Vertical Horizon:** FortiNAC requires a secure port for each VLAN that is expected to participate in disabling hosts by physical address. Define Cisco and Vertical Horizon secure ports outside of FortiNAC through their respective command line interfaces or local management. Configure secure ports on 3Com switches by selecting Secure Port Management from the device-specific pull-down in the Inventory.
- **Enterasys:** Enterasys switches do not require any special configuration in order to support Physical Address Filtering.
- **HP:** HP switches currently do not support Physical Address Filtering.
- **Nortel:** Nortel switches do not require any special configuration in order to support Physical Address Filtering.

Disable Hosts

- Hosts can be disabled manually from the Host View. See [Enable or disable hosts on page 230](#).
- Hosts can also be disabled when an event is generated that triggers an alarm. The alarm must be configured to perform an alarm action that disables the host. For more information on alarm actions, see [Add or modify alarm mapping on page 787](#).



If you delete a disabled host, the entry for that host's MAC address remains on the switch as disabled. Another user logging in through that host will not be able to access the switch. Be sure to enable the host before you delete it.

Example of host MAC addresses on a secure port

When the secure or static ports feature is used, the MAC addresses of disabled hosts are sent to the device. The device stores these MAC addresses in a list.

The list shown below displays all disabled hosts written to port12 (secure port) on a Cisco 2950 switch.

```
sw_chellis_24#show port-security
```

Secure Port (Count)	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation	Security Action

Fa0/12	120	3	0	Shutdown

Total Addresses in System : 3

Max Addresses limit in System : 1024

```
sw_chellis_24#show port-security address
```

Secure Mac Address Table

Vlan (mins)	Mac Address	Type	Ports	Remaining Age
20	0004.2353.2d19	SecureConfigured	Fa0/12	-
20	0009.5b83.e74c	SecureConfigured	Fa0/12	-
20	0009.5b89.0379	SecureConfigured	Fa0/12	-

Total Addresses in System : 3

Max Addresses limit in System : 1024

Secure port management

This option is not available for all devices. If the device supports Secure Ports the option appears in the right-click menu for the device.

1. Click **Network > Inventory**.
2. Right-click on the device and click **Secure Port Management**.
3. Click **Add**.
4. Click the port to be set as the secure port on the device.
5. Select the Group of hosts that will be given permission for this port if they are disabled.
6. Click **Add**.
7. The port and group are displayed in the Secure Port Management list.

Static port configuration

This option is not available for all devices. If the device supports Static Ports the option appears in the right-click menu for the device.

1. Click **Network > Inventory**.
2. Right-click on the device and click **Static Port Configuration**.
3. Click the port to be set as the static port on the device.
4. To Add, select **Add Static Port** from the drop-down menu.
5. To Remove, select **Remove Static Port** from the drop-down menu.
6. Click **Apply**.

Credentials

When SNMP managed devices are selected from the menu tree in the Inventory, a Credentials tab displays in the right pane. Use this view to verify FortiNAC's communication with the device or modify the access settings used to connect.

Field	Definition
Validate Credentials	Tests the values entered in the device model against the device: • SNMP credentials • CLI credentials • SSL settings
SNMP Settings	
SNMP Protocol	Available options: • SNMPv1 • SNMPv2c • SNMPv3-AuthPriv • SNMPv3-AuthNoPriv
Security Strings	SNMPv1 Community String
User Name	Required for SNMPv3. User Name for access to the device. Recommended but not required.
Authentication Protocol	Required for SNMPv3. Available options are: • MD5 • SHA1 • SHA224 • SHA256 • SHA384 • SHA512 (Recommended)
Authentication Password	Required for SNMPv3. Specify password to match what the device is using.
Privacy Protocol	Required for SNMPv3-AuthPriv. Available options are:

Field	Definition
	• DES • Triple DES • AES-128 • AES-192 • AES-256 (Recommended) • AES-192 Cisco • AES-256 Cisco
Privacy Password	Required for SNMPv3-AuthPriv. Specify password to match what the device is using. Note: Ensure that passwords are at least 8 characters in length. Please note that longer passwords with repetitive strings may result in exactly the same key. For example, a password 'fortfort' will result in exactly the same key as password 'fortfortfort'.
CLI Settings	
User Name	The user name used to log on to the device for configuration. This is for CLI access.  The user account must have the appropriate permissions configured on the device. For network devices using API credentials, the User Name is the serial number of the appliance.
Password	The password required to configure the device. This is for CLI access. For network devices using API credentials, the Password is the REST API Key.
Enable Password	The enable password for the device. This is for CLI access. Note: Arista switches can be configured to require typing "enable" to enter enable mode, but no password is needed. For such configurations, populate this field with the # character.
Super Password	The super password required for access to more features on 3Com devices.
HWC Connect Port	Port for the External Captive Portal that was configured by the user on the device during the initial device setup. This port is required for FortiNAC to send commands to the device. Consult the manufacturer for assistance in locating this port number.

Field	Definition
Use Public Key Authentication (if available) (vF 7.6.2 and greater)	Disabled by default (overrides set via CLI are honored). Enable or disable Public SSH key authentication for the device model. Some devices (such as the FortiGate) fail SSH login if the FortiGate and the FortiNAC Public Key Authentication settings are not matched. Example: Public Key Authentication is enabled in the FortiNAC device model but disabled in the FortiGate.
Telnet/SSH Connection Timeout (Sec)	Used to determine how long to wait to connect and/or establish a Telnet/SSH session for this device. When disabled (default), the global setting " Telnet/SSH Connection Timeout (Sec) " applies. See Network device .
CLI Command Timeout (Sec)	Used to determine how long to wait for a CLI response (prompt, show commands, etc) for this device. When disabled (default), the global setting " Telnet/SSH Connection Timeout (Sec) " applies. See Network device .
Protocol types	
Telnet	Use Telnet to log on to the device for configuration.
SSH1	Use SSH1 to log on to the device for configuration. See SSH Algorithm Support on page 70 .
SSH2	Use SSH2 to log on to the device for configuration. See SSH Algorithm Support on page 70 .
Use SSH Public Key Authentication	Check on this setting to activate SSH Public Key Authentication and show other related settings.
Device Key ID	Choose a SSH Public Key slot to store the SSH Public Key
SSH Public Key	Choose the SSH Public Key that will be used for SSH Public Key Authentication that will be used for authentication between FortiGate and FortiNAC. Click View Public Key to view the actual Public key. Make sure to click Save first, and then click Validate Credentials to ensure the SSH key is stored onto FortiGate. For more information on SSH Key Management, please see SSH Key Management on page 947.
API Key	
API Key	Enter then API Key generated on FortiGate to allow FortiNAC to make API calls in communicating with FortiGate. API Key can also be entered in the following two ways: 1. In Network > Inventory > select a FortiGate device > Credentials tab. 2. In Network > Inventory and click Add to add a FortiGate device. To generate a FortiGate API key on FortiGate, go to System > Administrator and generate a API Key using REST API Admin user. Make sure to click Save first, and then click Validate Credentials to verify FortiNAC is able to communicate with FortiGate through the API key.

Field	Definition
Port	Enter the FortiGate HTTPS port number.
SSL Settings (vF7.2.5 and greater FortiGate Models Only)	Offers enhanced security for communicating with network devices where FortiNAC uses the REST API. FortiNAC will not communicate with the device unless the SSL connection is considered "secure". The public key in the certificate must be signed by a trusted certificate authority (CA) known to FortiNAC. If FortiNAC does not trust the connection, clicking the Validate Credentials button will display "Certificate is not trusted".
View Certificate	View details for the certificate with the option to import if not already trusted by FortiNAC. When a certificate is imported, it is listed as a "General Trusted CA" certificate target under the Trusted Certificates view.
Device Certificate Verification	Toggle to enable/disable SSL certificate verification with this device. When enabled, the digital certificate presented by the device must be signed by a trusted certificate authority (CA). Important: Prior to enabling this option, ensure the CA certificate is listed as a "General Trusted CA" certificate target under the Trusted Certificates view. See Trusted Certificates.
Hostname Verification	Available option when Device Certificate Verification is enabled. Toggle to enable/disable hostname verification with this device. Adds an additional layer of security. The digital certificate presented by the device must contain the IP or hostname of the device in the subject alternative name (SAN) or the common name (CN). The SAN takes precedence and is checked first.

Ports view

When you select an item from the menu tree in the Topology, a Ports tab displays in the right pane. This view shows all the ports within the customer, container or device selected and the status of each port. For example, if you select a container, the Ports tab displays all of the ports on all of the devices that reside inside the selected container. If you select a device, all of the ports for that device are displayed.

You can also view the adapters/hosts and port changes for a selected port by clicking Show Details Panel. This panel provides direct access to the information found in the Connection Details and Port Changes Views for the selected port, allowing you to quickly view and modify adapters that are connected to the port. See [View connection details on page 357](#) and [Port changes on page 455](#) for information about the fields contained in these tabs.

Ports or interfaces are displayed in the order in which they appear in the interface table on a device. Depending on the device and its configuration, ports may not display in order numerically or alphabetically. When hosts are connected to a

port, icons are displayed to indicate the type of host that is connected and its status. You can update the Ports view for the selected device.

When you select a supported wireless device from the menu tree, Ports and SSIDs tabs are displayed in the right pane. This view shows all of the SSIDs on the device; however, it does not show when hosts are connected. If an SSID has been removed from the device, it is displayed in red on the SSIDs tab. The configuration information for that SSID remains in the database until it is deleted manually. When FortiNAC resynchronizes with the device, all SSIDs that exist on the device are displayed. If an SSID was deleted from FortiNAC, but still exists on the device, it reappears during resynchronization. See [SSID view on page 365](#).

See [Icons on page 44](#) for additional information.

Settings

Field	Definition
Status	Icon reflecting the port status on the device. See Icons on page 44 for additional information on each icon. When a registered host is present, the status is updated via L2 polling. If no host is registered (rogue host or no host), the status updates immediately.
Label	Internal ifname of the port. Unassigned: Created on FortiGate models. This interface is utilized when: - FortiGate wireless traffic (FortiWiFi or FortiAP) is detected on SSIDs in tunnel mode. - SSID is configured without a VLAN
Name	Default name displayed for the port is comprised of the sysName of the device, the ifName and, in curly braces, the ifAlias or Port Description. All of this information is read from the switch. For example, Cisco_2600 Fa/07 {Library Front Desk}, where Cisco_2600 is the system name of the device, Fa/07 is the ifName and {Library Front Desk} is the Port Description.
IP address	IP address of the device containing the port.
Interface ID	Internal ifIndex of the port.
Default VLAN	Default VLAN for the port read from the device.
Current VLAN	VLAN where the port has been placed based on the network access policy for the connected host or device .
Notes	User specified notes about the selected port. Notes are entered in Port Properties . See Port properties on page 360 .
Device	Name of the device containing the port.
Virtualized Device	Name of the VDOM containing the port. See FortiGate Multitenancy Integration Guide for details
Connection State	Connection State Defines the state and type of device connected to this port. View the icon in the Status column for additional information. Note: As of vF 7.6.3, the processing of a link-down trap will clear the connection state of the port by default. States include: All Uplinks: Displays ports that have a connection status of any uplink type.

Field	Definition
	• Device: Device is connected to this port. • Disabled Phone: Phone is connected and has been disabled. • Disabled Registered Host: Registered host is connected and has been disabled. • Disabled Rogue Host: Rogue host is connected and has been disabled. • Disabled User: User is connected and has been disabled. • Learned Uplink: Uplink mode has been set as Dynamic and a device that is modeled in FortiNAC is connected on the port. See Port uplink types on page 365 • Multiple Hosts: More than one host is connected on the port. • Not Connected: Nothing is connected to this port. • Not Uplink: Port is not an uplink. This is either because the Uplink Mode is dynamic and the conditions for FortiNAC to set it to an uplink have not been met, OR the mode has been set as Never Uplink. See Port uplink types on page 365 • Phone: An IP Phone is connected. • Registered AtRisk Host: Known host that has failed a scan or has been manually marked AtRisk is connected. • Registered Host: Known host is connected. • Rogue AtRisk Host: Unregistered host that has failed a scan or has been manually marked AtRisk is connected. • Rogue Host: Unknown host is connected. • Threshold Uplink: Uplink mode has been set as Dynamic and FortiNAC has determined that the number of MAC addresses on the port exceeds the System Defined Uplink count. See Port uplink types on page 365 • Unauthenticated Host: Host that is registered but has not authenticated is connected. • User: Authenticated user is connected. • User Defined Uplink: Uplink Mode has been configured as Always Uplink. See Port uplink types on page 365 • WAP Uplink: Wireless Access Point is connected to the port causing port to be set as an uplink. See Port uplink types on page 365
Current CLI	Name of the CLI configuration currently applied to the port.
Admin Status	Indicates whether the port has been administratively disabled or enabled in FortiNAC. The Admin Status column updates immediately, the change is pushed to the device, and the Status column reflects the device state after the next L2 poll.
Operational Status	Indicates whether a port is currently operational and connected to a device or not.
Enforcement Status	Display all types of Enforcement currently applied to a port based on its group membership, or Unenforced if it doesn't belong to any enforcement group. If the port has "Temporary Port Exception" configured, display the time details of the unenforcement status.
Last Modified By	User name of the last user to modify the port.
Last Modified Date	Date and time of the last modification to this port.
Right click options	
Show/Hide Details Panel	Shows/hides an additional panel showing adapters/hosts and port changes for the selected port. This information can also be found in the Connection Details and Port Changes Views.

Field	Definition
Connection Details	Displays connection details for the selected port. See View connection details on page 357 .
Group Membership	Displays port group membership, which allows you to view and modify the groups in which this port is a member. See Group membership on page 360 .
Port Changes	Opens the Port Changes View. See Port changes on page 455 .
Port Properties	Opens Port Properties for the selected port. See Port properties on page 360 .
Role Membership	Displays the list of roles in which the port is a member. See View role membership on page 332 .
Set Temporary Port Exception	Open a window for the users to set the start and end time of port exception. Also, the number of ports selected for this setting is shown. By default, "start time" is set as 1 minute after the current time.
Cancel Temporary Port Exception	Available when the select ports have "Set Temporary Port Exception" configured.
Select Device In Tree	Locates the selected device in the tree on the right and highlights it.
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746 .
 You must have permission to view the admin auditing log. See Add an administrator profile on page 139.	
Show Events	Displays events for the selected port.

Update ports view

The Ports View for configured devices that have been added to the Inventory does not initially contain the current host information for each port. FortiNAC must go out to the device and read the current host information. This is typically done automatically based on the polling options configured for the device, but you can also poll the device manually.

1. Click **Network > Inventory**.
2. Expand the container where the device is located.
3. Right-click the device and select **Polling > L2 (Hosts) Information**.

FortiNAC reads the host information from the device and updates the Ports tab in the right pane. The [Icons on page 44](#) contains descriptions of the icons shown in the Ports view.

View connection details

Connection Details displays information about the host connected on the selected port. The description will vary depending on the element connected. Status is represented by an icon. For a legend of status icons, see the [Icons on page 44](#).

1. Click **Network > Inventory**.
2. Expand the container where the device is located.
3. Select a device.
4. In the Ports tab on the right, right-click on a port and select **Connection Details**. The connection details are displayed.
5. Click the icon to view the information for the host connected to the port. This takes you to the **Adapter Properties** window for this host. See [Properties on page 221](#) for additional information.

Settings

Field	Description
Name	Name of the switch and port to which the host or device is connected.
Connected Elements	Number of interfaces connected to this port.
Devices	
Status	Displays one of several pingable icons indicating the type of host connected to this port. Pingables in the Devices table are managed only in the Topology. See the Icons on page 44 for information on each device icon.
Description	A description of the connected device. This field may contain any one of the following: • Vendor name • Hardware type • IP address
IP address	IP address of the device connected to this port.
Physical Address	MAC address of the device connected to this port.
Vendor Name	Vendor associated with the device's MAC address. Determined based on the vendor OUI's stored in the FortiNAC database.
Hosts	
Status	Displays the Adapter icon for the selected connection. If the icon is green, the adapter is connected. Click on the icon to go to Adapter Properties. See Properties on page 240 .
Host Status	Displays the Host icon for the selected connection. Host state is indicated by the icon displayed. See the Icons on page 44 for information on each state. Click on the icon to go to Host Properties. See Properties on page 221 .
IP address	IP address of the adapter connected to this port.
Physical Address	MAC address of the device connected to this port.
Vendor Name	Vendor associated with the host's MAC address. Determined based on the vendor OUI's stored in the FortiNAC database.
Host Name	Name of the connected host.
Registered To	User ID and name of the user to whom this host is registered. If a host is registered by host name, this field will be blank.
Logged On User	User ID and name of the user that is currently logged onto this host.

Add ports to groups

Ports on your network can belong to groups. Group membership can be viewed from **Groups** or by selecting the port in the Inventory.

1. Click **Network > Inventory**.
2. Expand the container where the device is located.
3. Select a device.
4. In the **Ports** tab on the right, use Ctrl-click or Shift-click to select the records you wish to add to the group.
5. Right-click on the ports and select **Add Ports To Groups**.
6. To add the port to a group, click the box next to the group name and then click **OK**.
7. To create a missing group:
 - a. Click **Create Group**.
 - b. Enter a group name.
 - c. If the new group should be a sub-group of an existing group, enable the **Parent Group** option and select the appropriate group from the list.
 - d. **Description** is optional.
 - e. Click **OK** to save the new group.
8. Click **OK** to save your group selections.

If an item is placed in a subgroup, it can only be removed when viewing the membership of that subgroup. It cannot be removed from the parent group containing the subgroup.

For example, the L2 network devices group contains the wired devices and wireless devices subgroups. The wired devices subgroup contains four 3COM switches. The wireless devices subgroup contains two Cisco switches. The L2 network devices group membership list shows all six switches, but to remove one of the 3COM switches you must go to the wired devices membership list.

Modify multiple ports

You can modify multiple ports on your network at the same time.

1. Click **Network > Inventory**.
2. Expand the container where the device is located.
3. Select a device.
4. In the **Ports** tab on the right, use Ctrl-click or Shift-click to select the records you wish to modify.
5. Right-click on the ports and select **Modify Properties**.
6. Select the **Admin Status** for the ports.
7. Select the **Uplink Mode** for the ports.

Mode	Description
Dynamic	Allows FortiNAC to set the port as an uplink when the threshold for connections is reached. If the MAC address on the port is that of a switch that is modeled in the Inventory, the port is set as an Uplink.

Mode	Description
Clear	Check this box to clear all dynamic uplink settings for this port. Settings are cleared when you click Apply . Once the settings are cleared the check mark is removed from the Clear box by FortiNAC.
Always Uplink	Sets the port to always be an uplink.
Never Uplink	Sets the port to never be an uplink.

8. Select the check boxes next to **Current VLAN** and **Default VLAN** and enter the values.
9. Click **OK**.

Group membership

Ports on your network can belong to groups. Group membership can be viewed from the Groups View window or by selecting the port in the Inventory.

1. Click **Network > Inventory**.
2. Expand the container where the device is located.
3. Select a device.
4. In the **Ports** tab on the right, right-click on a port and select **Group Membership**.
5. Check marks indicate that the port is a member of the group.
6. To add the port to a group, click the box next to the group name and then click **OK**.
7. To remove the port from a group, click to uncheck the box next to the group name and then click **OK**.
8. To create a missing group:
 - a. Click **Create Group**.
 - b. Enter a group name.
 - c. If the new group should be a sub-group of an existing group, enable the **Parent Group** option and select the appropriate group from the list.
 - d. **Description** is optional.
 - e. Click **OK** to save the new group.
9. Click **OK** to save your group selections.

Remove ports from multiple groups

1. Click **Network > Inventory**.
2. Expand the container where the device is located.
3. Select a device.
4. In the **Ports** tab on the right, use Ctrl-click or Shift-click to select the records you wish to modify.
5. Right-click on the ports and select **Remove Ports from Groups**.
6. Select the check box for each group you wish to remove the ports from.
7. Click **OK**.

Port properties

View and configure the default network access settings for the selected port.

1. Click **Network > Inventory**.
2. Expand the container where the device is located.
3. Select a device.
4. In the Ports tab on the right, right-click on a port and select **Port Properties**.
5. The **Port** option is displayed.
6. Use the table below to make any desired changes. Click **OK** to save.

Settings

Mode	Description
Name	The default name displayed for the port is comprised of the sysName of the device, the ifName and, in curly braces, the ifAlias or Port Description. All of this information is read from the switch. For example, Cisco_2600 Fa/07 {Library Front Desk}, where Cisco_2600 is the system name of the device, Fa/07 is the ifName and {Library Front Desk} is the Port Description.  Use only letters, numbers and hyphens (-) when creating port descriptions. Other characters, such as #, may prevent FortiNAC from communicating properly with the device.
Interface ID	Internal ifIndex of the port.
IP Address	IP address of the device containing the port.
Physical Address	Switch port MAC address
Admin Status	Select On or Off .
Connection State	Defines the state and type of device connected to this port. See Ports view on page 354 for a list of connection states.
Uplink Mode	• Dynamic: Allows FortiNAC to set the port as an uplink when the threshold for connections is reached. If the MAC address on the port is that of a switch that is modeled in the Inventory, the port is set as an Uplink. • Clear: Check this box to clear all dynamic uplink settings for this port. Settings are cleared when you click Apply. Once the settings are cleared the check mark is removed from the Clear box by FortiNAC. • Always Uplink: Sets the port to always be an uplink. • Never Uplink: Sets the port to never be an uplink.
Current VLAN	VLAN where the port has been placed based on the network access policy for the connected host or device.

Mode	Description
	To modify, enter the value for the Current VLAN and select OK. A warning message appears. Click Yes to confirm that you wish to modify the Current VLAN and save the port properties. Important: Manually changing VLANs should be done through the Administration UI instead of the switch itself. For details, see article Best practice for manually changing VLANs on managed switches
Default VLAN	Default VLAN for the port read from the device. To modify, enter the value for the Default VLAN and select OK.
CLI Configuration	Displays the most recent CLI configuration that has been applied to this port.
Port Mode (v9.4.6/7.2.6 and greater)	Current mode of the port. Possible modes include: • 8021x: Using RADIUS 802.1x authentication on this port. The mode is triggered when a RADIUS 802.1x authentication request is received on the port. Use the Clear checkbox to reset mode to NORMAL. • RADMAC: Using RADIUS MAC authentication on this port. The mode is triggered when a RADIUS MAC authentication request is received on the port. Use the Clear checkbox to reset mode to NORMAL. • NORMAL: RADIUS authentication is not in use on this port. Clear checkbox: Resets mode to NORMAL.
Dot1x Auto Registration	Disabled by default. Automatic registration of a host based upon the user's 802.1x authentication with the RADIUS server. Upon successful 802.1x authentication, FortiNAC registers the host to the authenticated user prior to the network policy being determined. Requirement: RADIUS request from Controller/Access Point must contain RADIUS Attribute 30 and include the port value
Port Changes	Click to display the Port Changes View .
Group Membership	Click to display Port Group Membership to view and modify the groups in which this port is a member. Group Membership only appears if the user has permission to view group membership. If the user has permission to view but not modify group membership, the user cannot save changes to group membership.

Temporary port exception

The Temporary Port Exception Group is a system-defined group introduced in FortiNAC F 7.6.1 to reduce administrative overhead when configuring port exceptions. This feature enables users to specify certain ports that should be exempt from enforcement during a predefined exception time.

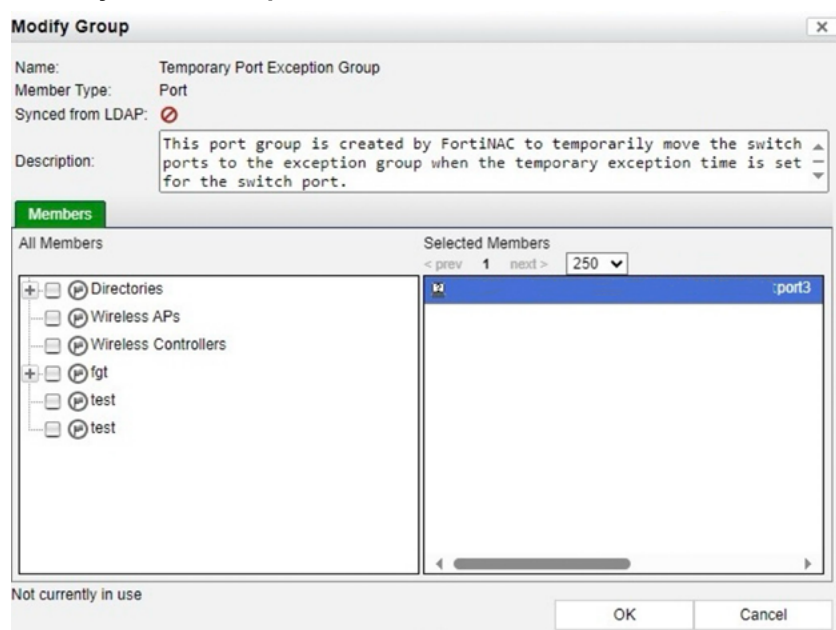
During this exception period, devices connected to these ports will have no policy enforcement. Once the exception period expires, the ports are automatically removed from the Temporary Port Exception Group and revert to their original enforcement groups, restoring the previously applied policies.

This new feature provides greater flexibility in managing port exceptions, while minimizing manual configuration efforts and ensuring seamless transitions back to standard enforcement.

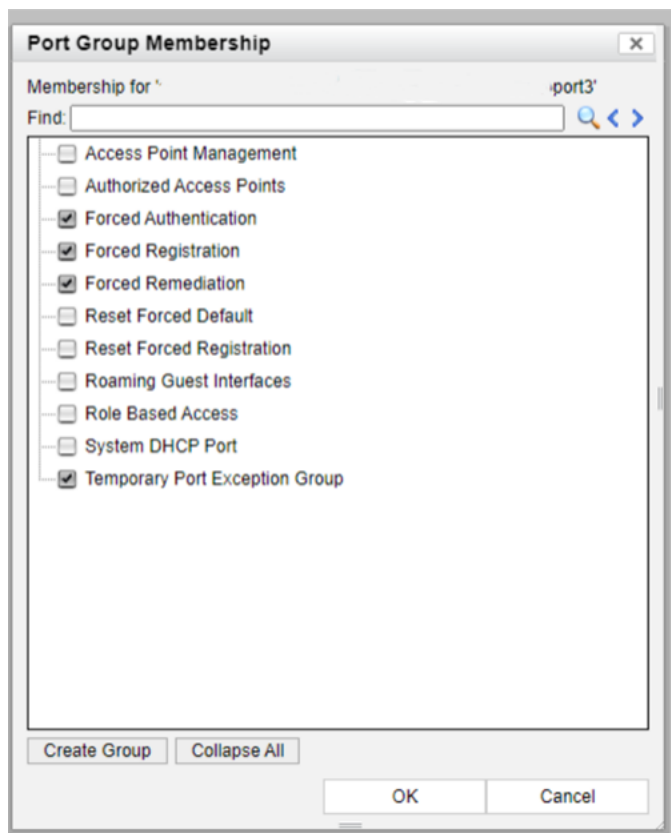
Note: “Temporary Port Exception” configuration applies only to switch ports in FortiNAC.

Configuration Steps

1. To configure a port for an exception, go to **Network > Inventory > Ports View** and right click on the port(s) and select **Set Temporary Port Exception**.
2. Set the start and end time.
3. Once the configuration is saved, users can view the port's membership in the **Temporary Port Exception Group** under **System > Groups**.



Additionally, in **Network > Inventory**, the **Group Membership** window for the configured ports will indicate Temporary Port Exception Group as selected.



- To view the details of the exception configuration, navigate to **Inventory > Ports View**, where the **Enforcement Status** column for the corresponding ports will display their current enforcement state, along with details of the upcoming unenforcement time.

Ports													
Filter													
Add Filter: Select Update													
Select All Hide Details Panel													
Ports: Displayed: 8 Total: 8													
Status	Device	Label	Name	IP Address	Connection State	Default VLAN	Current VLAN	Admin Status	Operational Status	Enforcement Status	Notes	Last Modified By	Last Modified Date
FG	465	port1	FGV	1port1	1 1.1	Learned UpLink	1	On	Link Up	Unenforced		SYSTEM	2024/09/10 21:36:27
FG	465	port2	FGV	1port2	1 1.1	Not Connected	1	On	Link Up	Unenforced		SYSTEM	2024/09/10 21:55:00
FG	465	port3	FGV	1port3	1 1.1	Rogue Host	1	On	Link Up	Unenforced from 2024/09/10 22:03:30 to 2024/09/10 22:13:30	Authentication, Registration, Remediation	SYSTEM	2024/09/10 22:02:33
FG	465	port4	FGV	1port4	1 1.1	Not Connected	1	On	Link Up	Unenforced		SYSTEM	2024/09/10 21:36:27
FG	465	port5	FGV	1port5	1 1.1	Not Connected	1	On	Link Up	Unenforced		SYSTEM	2024/09/10 21:36:27
FG	465	port6	FGV	1port6	1 1.1	Not Connected	1	On	Link Up	Unenforced		SYSTEM	2024/09/10 21:36:27
FG	465	port7	FGV	1port7	1 1.1	Not Connected	1	On	Link Up	Unenforced		SYSTEM	2024/09/10 21:52:30
FG	465	port8	FGV	1port8	1 1.1	Not Connected	1	On	Link Up	Unenforced		SYSTEM	2024/09/10 21:36:27

During the exception period, the **Enforcement Status** for ports in the Temporary Port Exception Group will show the end time of the current unenforcement period, providing clear visibility into the temporary status change.

Ports													
Filter													
Add Filter: Select Update													
Select All Hide Details Panel													
Ports: Displayed: 8 Total: 8													
Status	Device	Label	Name	IP Address	Connection State	Default VLAN	Current VLAN	Admin Status	Operational Status	Enforcement Status	Notes	Last Modified By	Last Modified Date
FG	465	port1	FGV	1port1	1 1.1	Learned UpLink	1	On	Link Up	Unenforced		SYSTEM	2024/09/10 21:36:27
FG	465	port2	FGV	1port2	1 1.1	Not Connected	1	On	Link Up	Unenforced		SYSTEM	2024/09/10 21:55:00
FG	465	port3	FGV	1port3	1 1.1	Rogue Host	1	On	Link Up	Unenforced until 2024/09/10 22:13:30		SYSTEM	2024/09/10 22:02:33
FG	465	port4	FGV	1port4	1 1.1	Not Connected	1	On	Link Up	Unenforced		SYSTEM	2024/09/10 21:36:27
FG	465	port5	FGV	1port5	1 1.1	Not Connected	1	On	Link Up	Unenforced		SYSTEM	2024/09/10 21:36:27
FG	465	port6	FGV	1port6	1 1.1	Not Connected	1	On	Link Up	Unenforced		SYSTEM	2024/09/10 21:36:27
FG	465	port7	FGV	1port7	1 1.1	Not Connected	1	On	Link Up	Unenforced		SYSTEM	2024/09/10 21:52:30
FG	465	port8	FGV	1port8	1 1.1	Not Connected	1	On	Link Up	Unenforced		SYSTEM	2024/09/10 21:36:27

Once the exception period expires, the ports are automatically removed from the Temporary Port Exception Group and revert to their original enforcement groups, restoring the previously applied policies.

Note: Once an exception is set for a port, no additional exceptions can be applied to the same port. However, users can cancel the current exception at any time and create a new exception with updated time parameters if necessary. Users

are also allowed to cancel the configured exception at any time by simply right clicking on the port and select **Cancel Port Temporary Exception**.

Port uplink types

Uplinks disable management of the port, which means access is no longer controlled from the port.

Learned Uplink: The Uplink mode has been set as Dynamic and a device that is modeled in FortiNAC is connected on the port. All hosts read on this port are ignored.

Threshold Uplink: The Uplink mode has been set as Dynamic and FortiNAC has determined that the number of MAC addresses on the port exceeds the System Defined Uplink count. All hosts read on this port are ignored.

User Defined Uplink: The Uplink Mode has been configured as Always Uplink. These are ports the user knows are uplinks, but will not be converted to a Learned or Threshold Uplink. All hosts read on this port are ignored.

WAP Uplink: A Wireless Access Point (WAP) is connected to the port, causing the port to be set as an uplink. These access points represent controller-managed devices.

A WAP Uplink controls access from this port for the AP only. The port is managed based on the physical address of the AP. Port management for all other hosts is disabled.

After an L2 Poll, the Uplink status is removed from all WAP uplinks when the MAC address for the AP is disconnected from the port.

SSID view

When you select a supported wireless device from the menu tree in the Topology, Ports and SSIDs tabs are displayed in the right pane. This view shows all of the SSIDs on the device; however, it does not show when hosts are connected. If an SSID has been removed from the device, it is displayed in red on the SSIDs tab. The configuration information for that SSID remains in the database until it is deleted manually. When FortiNAC resynchronizes with the device, all SSIDs that exist on the device are displayed. If an SSID was deleted from FortiNAC, but still exists on the device, it reappears during resynchronization.



FortiNAC does not display SSIDs for all wireless devices. Refer to [WLAN Management](#) and for additional information.

See [Icons on page 44](#) for additional information.

Settings

Field	Definition
Add Filter	Allows you to select a field from the current view to filter information. Select the field from the drop-down list, and then enter the information you wish to filter.
Update Button	Click to update the data in the table.
Table columns	
Name	The SSID name.

Field	Definition
Description	A description of the SSID that can be edited through SSID Configuration. To access SSID Configuration, double click on any SSID to edit the description field.
Container	Container where the device that is broadcasting the SSID resides. Containers are used to group devices.
Device	Name of the device that is broadcasting the SSID.
Virtualized Device	Name of the VDOM containing the SSID.
RADIUS	Indicates whether the SSID inherits the RADIUS server settings from its parent device, or if the settings are customized in the SSID Configuration.
Network Access	Indicates whether the SSID inherits the network access or VLAN/role settings of its parent device, or if the settings are customized in the SSID Configuration.
Primary RADIUS Server	The RADIUS server used for authenticating users connecting to the network through this SSID. See RADIUS on page 375 for information on configuring your RADIUS servers.
Secondary RADIUS Server	If the primary RADIUS server fails to respond, this RADIUS server is used for authenticating users connecting to the network until the primary RADIUS server responds.
Default	The Default VLAN value is stored in the FortiNAC database and is used when the VLAN is not determined by another method, such as a network access policy. Typically, if a VLAN is specified as the Default, it is the VLAN used for "normal" or "production" network access. It will be used for all the untagged (non-uplink) ports on the device.
Dead End	The dead end VLAN for this SSID. Isolates disabled hosts with limited or no network connectivity from the production network.
Registration	The registration VLAN for this SSID. Isolates unregistered hosts from the production network during host registration.
Quarantine	The quarantine VLAN for this SSID. Isolates hosts from the production network who pose a security risk because they failed a scan defined in an endpoint compliance policy.
Authentication	The authentication VLAN for this device. Isolates registered hosts from the Production network during user authentication.
Right click options	
Delete	Deletes the selected SSID.
Group Membership	Displays port group membership, which allows you to view and modify the groups in which this port is a member. See Group membership on page 360 .
SSID Configuration	Opens the SSID configuration on page 367 window. If multiple SSIDs are selected simultaneously, the Modify SSID Configuration window opens.

Field	Definition
Select Device In Tree	Locates the selected device in the tree on the right and highlights it.
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746 .
 You must have permission to view the admin auditing log. See Add an administrator profile on page 139 .	

SSID configuration

SSIDs on some wireless devices can be configured with VLAN/Role settings that are different than those of the parent device. This option allows you to provide different treatment for each SSID. For example, you can have an SSID that provides only Internet access for guests and a separate more secure SSID that requires authentication for staff.



In an environment where there are multiple SSIDs that have the same name, FortiNAC cannot manage those SSIDs individually. Make sure that SSIDs do not have the same name.

1. Click **Network > Inventory**.
2. Expand the container where the wireless device is located.
3. Select a device.
4. In the right pane, select the **SSID tab**.
5. Right-click on the SSID and select **SSID Configuration**. To modify multiple SSIDs simultaneously, see [Modify multiple SSIDs on page 370](#).
6. Use the table below to configure the SSID.
7. Click **OK** to save.

Settings

Settings	Description
RADIUS	
Use Inherited RADIUS Server Definitions from Device	If enabled, the SSID inherits the RADIUS server settings of its parent device.
Use Custom Settings	If enabled, allows you to set the default primary and secondary RADIUS servers to the servers indicated in parentheses and set the RADIUS Secret.
Primary RADIUS Server	The RADIUS server used for authenticating users connecting to the network through this SSID. See RADIUS on page 375 for information on configuring your RADIUS servers.

Settings	Description
Secondary RADIUS Server	If the primary RADIUS server fails to respond, this RADIUS server is used for authenticating users connecting to the network until the primary RADIUS server responds.
RADIUS Secret	The Secret used for RADIUS authentication. Click the field to add or modify the RADIUS Secret.  The RADIUS Secret used must be exactly the same on the wireless device, on the RADIUS server and in the FortiNAC software under RADIUS Settings and Model Configuration.
Show/Hide Button	Allows you to display or hide the RADIUS secret.
Enable RADIUS authentication for this device	When selected, FortiNAC will process RADIUS requests from the device.
Mode	The RADIUS Authentication Mode to be used when a RADIUS request is received from the modeled device. Local: Use the Local RADIUS server. Enter the RADIUS Secret, and choose the attributes to be sent in the Accept packet. Proxy: Use the RADIUS Proxy. Optionally choose to override the RADIUS server to proxy to and enter the RADIUS secret.
Default RADIUS Attribute Group (Local RADIUS Option)	The default RADIUS Attributes to be sent for all accepted requests from this device. Hover over the group name to see what attributes and values will be sent. FortiNAC has pre-built attribute groups that can be used for most devices.
RFC5176 Mode settings	 See the RFC5176 CoA/Disconnect Message Cookbook for more details. RFC5176 Mode The RADIUS RFC5176 Mode to be used for dynamic authorization change, for example, an authenticated host switches VLAN. • System defined: Use the system defined RFC5176 settings (Disconnect message with default attributes) • Custom: Use custom RFC5176 settings. Port, message type and attribute group can be configured in sections below. • Multiple connection: Force the system to use the RFC5176 Message type and Attribute Groups under RFC5176 to build up the CoA/Disconnect message if certain conditions are satisfied. • Daisy chain: Configure FortiNAC to send unique attributes to the port if the hosts are daisy-chained.

Settings	Description
	RFC5176 Port The port that receives CoA and Disconnect messages. By default, it is 3799. RFC5176 message type Choose the type of message that will be sent during dynamic authentication change: CoA or disconnect message. RFC5176 attribute group Attributes that will be sent during dynamic authentication change.
Network access	
Use Inherited Network Access Policy from Device	If enabled, the SSID inherits the network access or VLAN/role settings of its parent device.
Use Custom Settings	If enabled, allows you to customize the network access policy instead of using the inherited policy from the device.
Access Enforcement	When Use Custom Settings is enabled, this set of drop-down menus works in conjunction with the Host States listed below to determine treatment for hosts when no VLAN/Role value is supplied or when access control is being enforced. Options include: • Deny: Host will be denied access to the network when it is in this state. For example, if the host is not registered and Registration is set to Deny, the host connection will be rejected.  Endpoints that have been denied access may continuously request access which can unnecessarily consume system resources. • Bypass: Host will be allowed access to the network when it is in this state. The host will be placed on the default VLAN/Role configured on the device for this port or SSID. For example, if Quarantine is set to Bypass, hosts that fail a scan and would normally be placed in Quarantine are placed in the default VLAN/Role on the device. • Enforce: Indicates that the host will be placed in the VLAN/Role specified in the Access Value column for this state.
Access Value	VLAN/Role where a host in this state should be placed when it connects to the network. If Enforce is selected in the Access Enforcement field you must enter a value in the Access Value field.
Dot1x Auto Registration	Enabled/Disabled per SSID (disabled by default). Automatic registration of a host based upon the user's 802.1x authentication with the RADIUS server. Upon successful 802.1x authentication, FortiNAC registers the host to the authenticated user prior to the network policy being determined. Requirements: • FortiNAC version 8.5.2 or higher

Settings	Description
	RADIUS request from Controller/Access Point must contain RADIUS Attribute 30 and include the SSID value
Additional RADIUS Attribute Group (Local RADIUS option)	For each Logical Network, you can choose to either use the default values only, or to append and overwrite with another attribute group. Hover over the group name to see what attributes and values will be sent. FortiNAC can send different DM or CoA messages for host switching to different VLANs according to the RFC5176 settings in Logical Network, since RFC5176 Settings in Logical network has higher priority than those in device level. See the CoA Cookbook.
Host state	
Default	The Default VLAN value is stored in the FortiNAC database and is used when the VLAN is not determined by another method, such as a network access policy. Typically, if a VLAN is specified as the Default, it is the VLAN used for "normal" or "production" network access. It will be used for all the untagged (non-uplink) ports on the device. Select None to use the default VLAN/Role configured on the device.
Dead End	The dead end VLAN for this SSID. Isolates disabled hosts with limited or no network connectivity from the production network.
Registration	The registration VLAN for this SSID. Isolates unregistered hosts from the production network during host registration.
Quarantine	The quarantine VLAN for this SSID. Isolates hosts from the production network who pose a security risk because they failed a scan defined in an endpoint compliance policy.
Authentication	The authentication VLAN for this device. Isolates registered hosts from the Production network during user authentication.

Modify multiple SSIDs

1. Click **Network > Inventory**.
2. Do one of the following:
 - Select the top level container.
 - Select a container where the wireless device is located.
 - Expand the container where the wireless device is located and select a device.
3. In the right pane, select the **SSID** tab.
4. Hold CTRL or SHIFT and click to select multiple SSIDs.
5. Right-click and select **SSID Configuration**.
6. Select **RADIUS**, **Network Access**, or both.

7. See [SSID configuration on page 367](#) for the settings to configure the SSIDs.



If you select an Access Value that is not supported on all devices associated to the selected SSIDs, a link appears that allows you to view which device or devices do not support the value. Changes to the SSID configuration will only be saved for the devices that support the selected Access Values. The SSID Configuration for the device or devices that do not support the selected Access Values will remain unchanged.

8. Click **OK** to save.

Virtualized Devices

The Virtualized Devices tab in the right pane displays all the virtual domains (VDOMs). Virtualized Devices will be accessible from the top-level of Inventory and from each container.

From this view, customers have the option to select multiple VDOMs at once for editing. Right clicking the device will provide options for Model Configuration, Add Virtualized Devices to Groups, and Set Model Configuration. To learn more about these options, see [Model configuration on page 338](#).

Note: For **Default Logical Network > edit** page in **SSID** or **Virtualized Devices**, there is no RFC5176 fields for the user to fill in; FortiNAC will use the settings in Device Level.

Modify Multiple Virtualized Devices

1. Click **Network > Inventory**.
2. In the **Virtualized Devices** tab, Ctrl-click or Shift-click to select the devices you wish to modify.
3. Right click the selected devices and select **Set Model Configurations**.
The number of devices you selected to be modified will show next to **Add Configuration Category**.
4. Select the **Configuration Categories** to modify from the drop down menu off **Add Configuration Category**.
See [Model configuration on page 338](#) for more details.

Group Virtualized Devices

1. Navigate to **Network > Inventory**.
2. In the Virtualized Devices tab, Ctrl-click or Shift-click to select the devices you wish to group.
3. Right click the selected devices and select **Add Virtualized Devices to Groups**.
4. Select or create a group to add the devices to. Click **OK**.

Send SSO Tag/Group Data to a FGT

FNAC supports the ability to send SSO tag/group data to one or more FortiGates for a variety of scenarios, including:

1. Hosts that appear as detected devices on a FortiGate wired interface.
2. Hosts that have a wired connection to a FortiLink FSW managed by a FortiGate.
3. Hosts that have wireless connections to a FortiGate through a FortiAP.
4. Hosts that have a VPN connection to a FortiGate.
5. Hosts that are connected anywhere in the network to a network device managed by FNAC.

6. Hosts that are running a FortiNAC Persistent Agent which is communicating to FNAC but are otherwise not seen by FNAC as connected to any managed network device.

Note: For scenario 6, the host must belong to a group that is selected in the "**Connect Hosts in Group when Agent Connects**" option. The group is not used by the other scenarios.

Setting up the SSO tag/group data

- Hosts for which you want to send SSO must belong in a group and the group must be selected to enable the new capability.
1. Navigate to **System > Groups**
 2. Create or Modify a group and add to it the hosts you wish to send SSO.
 3. Navigate to **System > Settings > Persistent Agent > Properties**.
 4. Select the group that was populated with your hosts under **Connect Hosts in Group when Agent Connects**.
Note: This step is for hosts that are running a FortiNAC Persistent Agent which is communicating to FNAC but are otherwise not seen by FNAC as connected to any managed network device.
 5. Navigate to **Policy & Objects > User/Host Profiles** and create a new User/Host profile and add your group to the **Who/What by Group** setting. You may add other criteria as desired to filter the hosts you wish to include.
 6. Navigate to **Policy & Objects > Network Access > Logical Networks** or **Network > Logical Networks**. Create a new Logical Network.
 7. Navigate to **Policy & Objects > Network Access > Configurations**. Create a new Network Access Configuration using the new Logical Network.
 8. Create a new Network Access Policy using the new Network Access Configuration and new User/Host Profile.
 9. Navigate to **Network > Inventory**. Select the FortiGate device to which you want to send SSO. Click the **Virtualized Devices** Tab for the Fortigate Device.
 10. Choose the VDOM value you want to configure. Double click or click **Model Configuration** to open a new window with settings to create or choose tags to send to the FGT for the given Logical Network created for your Network Access Policy.

Importing tag/groups into FortiGate

- FNAC must exist as a fabric connector on each FGT to which you want to integrate with SSO.
1. Navigate to **Security Fabric > Fabric Connectors**.
 2. Either create or edit the FortiNAC Tags object, and select the Refresh button. It may take several Refresh attempts but should result in importing all the Host group and tag information created within FNAC. You should see the values from the View button.
 3. Enable a setting on each FGT model within FNAC to force SSO data to be sent to that FGT. The setting must be configured from a command shell on the FNAC appliance. The `device` command can be used to show or set values. Use the command to set a "ForceSSO" attribute to "true" on the FGT models:
`device -ip 10.12.234.101 -setAttr -name ForceSSO -value true`

Note: This configuration is deprecated. See [Addresses on page 935](#) for creating network address objects and group objects for preferred configurations.

The FortiNAC tags connector under **Security Fabric > Fabric Connectors** is deprecated in FortiOS 7.0.4 and later. For upgrade support, the FSSO FortiNAC user type can still be configured in the CLI.

CLI example

```
config user fsso
  edit "NACKY-NAC"
    set type fortinac
    set server "192.168.20.8"
```

```
set password ENC
    r6Iz+hGTDzZMVYL95QX8lO/97skiXNZwPGoA0MrPWyi7iNRWlKLGQtTena9IPprqRks2LWarkQ
    zDXuAgLncdhVLut3tf2NYgIB9gFxnmn0xALL5qNjN120kLBSazg3n4XWXzsaKFcJD1FbE5a5dj
    ZMFaGjKcy+NPwLqTliEE8OfAFJWb1P7sf4pvaBZ15j7nJATBsw==
next
end
```

FortiOS 7.0.4 and later can communicate with FortiNAC over REST API once FortiNAC is authorized into the Security Fabric.

See [FortiNAC security fabric authorization](#) for more details about authorization.

See [Replace FSSO-based FortiNAC tag connector with REST API](#) for more information about FortiGate dynamic firewall addresses for FortiNAC tags.

Logical networks

Use logical networks to separate network access policies from device specific values. Each logical network has an access value, which is translated to the physical value of network infrastructure devices. FortiNAC uses this value to provision the appropriate network access. Using logical networks can simplify network policy management by reducing the number of required policies.

Once you create a logical network, you then assign access values on individual devices, then assign a network access configuration for the logical network.

In a FortiNAC Manager environment, you can create logical networks on the FortiNAC Manager and push this information to other managed FortiNAC appliances.

Configuring logical networks

You can create, modify, or delete all logical networks shown in the **Logical Networks** tab, including the pre-defined logical networks if they were added using the 'Add Predefined Network Access Policies' task during the guided installation.

Creating a logical network

1. Go to **Network > Logical Networks**.
2. Click **Create New**.
3. Enter a **Name** for the logical network.
4. (Optional) Enter a **Description**.
5. Click **OK**.

Modifying a logical network

1. Go to **Network > Logical Networks**.
2. Click the logical network and click **Modify**.
3. Modify the **Name** and/or **Description**.
4. Click **OK**.

Deleting a logical network

1. Go to **Network > Logical Networks**.
2. Click the logical network and click **Delete**.
You cannot delete a logical network that is currently in use. Click **In Use** to check if a logical network is in use.
3. Click **OK** to confirm.

Assigning access values and CLI configurations

You assign access values and CLI configurations to devices for each logical network, either by configuring a single device or configuring multiple devices at the same time.

Several default networks are shown as logical networks in the **Model Configuration** tab: **Default**, **Registration**, **Quarantine**, **Dead End**, **Authentication**, and **Voice**. These networks are configured as logical networks but do not appear in the **Logical Networks** tab.

Configuring a single device

1. Go to **Network > Inventory**.
2. Expand the container where the device is located.
3. Click the device and click the **Model Configuration** tab.
4. Under **Access**, use the drop-down list to set the access value for each logical network.
5. (Optional) Set **CLI Configuration Type** to **Port Based** or **Host Based**. Under **CLI**, use the drop-down list to set the configuration for each logical network.
6. Click **Save**.

Configuring multiple devices

1. Go to **Network > Inventory**.
2. Select the container where the devices is located.
3. In the **Devices** tab, click the devices while pressing **Ctrl**.
4. Right-click the devices and click **Set Model Configuration**.
5. Use the **Add Configuration Category** drop-down list to select a logical network.
6. Select **Access Value/VLAN** and assign a value.
7. (Optional) Select **CLI Configuration Type**, set type to **Port Based** or **Host Based**, and select a configuration.
8. Click **OK**.

Configuring network access policies

If you initialized network access policies to include the pre-defined sample configuration using the 'Add Predefined Network Access Policies' task in the guided installation, then the pre-defined logical networks are assigned network access policies. By default, these policies are disabled.

To assign logical networks using network access policies, see [Create or edit a policy](#).

RADIUS

Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

A RADIUS server enables external authentication for users connected to FortiNAC managed network devices. This type of server is often used in a wireless environment, but also used in wired environments supporting 802.1x authentication.

FortiNAC uses RADIUS authentication for several purposes including:

- Authenticating users attaching to managed network devices using 802.1x.
- Authenticating VPN users.
- Authenticating users accessing FortiNAC's own captive portal process.
- Authenticating administrators logging onto the FortiNAC system.

As of version 8.8, FortiNAC can be configured to authenticate RADIUS using external RADIUS server(s), the built-in local RADIUS server or a combination of both. There are two RADIUS Authentication modes available for determining how RADIUS requests are processed. These can be configured in FortiNAC on a per-device basis.

MAC Authentication Bypass (MAB)

When using MAB in a FortiNAC managed environment, it is necessary to configure the following components so that all can communicate successfully:

- Network devices
- FortiNAC

The above components must have the same RADIUS secret key value defined.

RADIUS Access-Requests from the device must contain:

- Calling-Station-Id
- User-Name
- User-Password

All 3 attributes must contain the same valid MAC Address.

802.1x environments

When using 802.1x in a FortiNAC managed environment, it is necessary to configure the following components so that all can communicate successfully:

- Network devices
- FortiNAC
- Production RADIUS server(s)

All the above components must have the same RADIUS secret key value defined. FortiNAC does not modify 802.1x packets as they pass from the network device through to the terminating RADIUS server.

The same requirement exists when using Domain mapping. For instance, many wireless devices that support 802.1x allow a RADIUS server definition for each configured SSID. In such an environment, if two users are connected to the same SSID but to different domains, the RADIUS secret used in both authentication requests would be identical. The users are both using the same RADIUS profile on the wireless device. Assuming FortiNAC were configured to use different terminating RADIUS servers for each domain, it would forward the requests and both servers would need to use the same secret value in order to validate the packets.

Order of precedence

When one or more RADIUS servers are used for authentication coupled with different methods of configuration, it can be difficult to determine which server will be used. The uses for RADIUS servers are as follows:

- Authenticating FortiNAC administrators.
- Authenticating network users accessing the network through a VPN.
- Authenticating network users who come in through the captive portal.
- Devices that have no RADIUS servers configured in the model configuration.
- Devices that have specific RADIUS servers configured in the model configuration.
- SSIDs that have no RADIUS servers configured and inherit from the parent device.
- SSIDs that have specific RADIUS servers configured.

Unless a specific RADIUS server is configured for a particular device or SSID, these options use the default primary and secondary RADIUS servers. However, if RADIUS server profiles are mapped to domains and the authenticating user's username contains a domain name prefix, then the RADIUS server mapped to the domain takes precedence. The order of precedence to determine which RADIUS server is used is as follows:

1. If domain mappings exist and an entry matches the domain prefix contained within the user name of a connecting user, then the RADIUS server mapped to the domain is used. Multiple servers can be mapped to a single domain. If the user is not found on the first RADIUS server in the list, FortiNAC checks each server mapped to the domain in turn until the user is found.
2. If a blank domain has been mapped and an authenticating user does not have a domain prefix in the user name, then the server or servers mapped to the blank domain are used.
If you create a domain mapping for a RADIUS server with a blank domain name this always takes precedence over the default primary and secondary RADIUS servers because all users who do not use domain name to log in will match this mapping.
3. If no domain mappings exist, the RADIUS server profile chosen for the originating SSID is used.
4. If no SSID mapping exists, the RADIUS server profile chosen for the originating device is used.
5. If no device specific server selection exists, the system-wide default primary and secondary server settings are used.

Configuration

This view is used to configure FortiNAC as the 802.1x EAP termination point.

Note:

- Requires Server Certificate to be installed for EAP authentication. For installation instructions see [Certificate management on page 828](#).

- FortiNAC can be configured to authenticate RADIUS using either the built-in local RADIUS server, external server (s) or a combination of both. To configure FortiNAC to proxy 802.1x packets to an external RADIUS server for EAP termination, see [RADIUS on page 375](#)
- Multiple server configurations is supported.

Field	Description
Service Info	
Status	Displays the current server status. • Enabled Status: Displays ◦ Enabled if the service is configured to run on boot. ◦ Disabled if the service is not configured to run on boot • Running Status: Displays ◦ Running if the service is running ◦ Stopped if the service is not running
Toggle Service Status	Enable/Disable processing of local RADIUS requests
Details & Logs	Displays the radius service log, the radius specific output of the FNAC server log, and the system journal. The view will tag important failure messages in red, and includes a filter control to both show only lines w/ the specified string (the 'Filter' button), or to color lines containing the specified string (the 'Mark' button), to keep context.

RADIUS Service Details

This view shows FortiNAC server logs (the most recent 3000 lines). Can be used for both Local and Proxy Virtual Server configurations. These logs do not apply to Legacy Proxy configurations.

- **Service Status:** Shows additional details of the state of the RADIUS service beyond the status field in the main view
- **Service Log:** Shows the debug information for the RADIUS service. The place to start when authentication is not working as expected.
Note: In most cases, the 'Service Log Level' should be set to Normal for the best troubleshooting information.
- **Server Log:** FNAC server log. Useful to debug post-auth related problems such as incorrect or missing response values, or a post-auth Deny being returned unexpectedly.
- **Systemd Journal:** OS journal output that shows helpful information when the service will not start for some reason (missing / corrupt configuration files, certificates, etc).
- **Network Access:** Displays all Access-Requests and the corresponding Access-Accept or Access-Reject, and the attributes in the request/reply or cause for the Access-Reject.

Logs can be filtered using the controls at the top of the view.

- **Filter Button:** Shows only lines containing the filter string
- **Mark Button:** Shows the full log output but highlights lines containing the filter string in blue for context. This can be used multiple times to highlight

Field	Description
	additional strings • Clear Button: Resets the filter • Previous/Next Buttons: Will auto scroll and select matches for the specified filter string • Show Flagged Errors Only: Shows only lines that have been flagged in red as common problem.
General Settings	
Authentication Port	RADIUS service will listen for authentication requests on the specified port. This is typically port 1812 or 1645. Note: For Eduroam enabled networks, port 1812 must be used. Important: If external RADIUS servers are also defined, the authentication port must be set to a different value than the RADIUS proxy ports.
Proxy Accounting	If enabled, the RADIUS service will listen for accounting packets on the specified authentication port +1. As the authentication port is typically 1812 or 1645, this is typically 1813 or 1646. FortiNAC proxies the packets to a customer-owned (external) RADIUS server. In some RADIUS integrations, FortiNAC can also process the accounting packets. Refer to the integration guides in the Document Library for details. Note: RADIUS accounting is only supported by virtual servers of type "Proxy". It is not supported for Local virtual servers.
Proxy MAB Requests	If enabled, proxy virtual servers will proxy all requests, including MAC authentication Bypass (MAB). When disabled, proxy virtual servers will only proxy 802.1x requests, and will process MAB requests locally.
Activity Monitoring	Enable activity monitoring to track authentication statistics. This exposes a new tab in Network > RADIUS > Activity tab. See Activity. Alternatively, add the RADIUS widget to a dashboard panel to view current, timeline or historical comparison data. The timeline and historical comparison views will become useful after activity monitoring has been enabled for some time.
Authentication Failure Events	Enable to generate an event for each authentication failure. This information can be exported using an external log receiver such as FortiSIEM or FortiAnalyzer. Independent of Activity Monitoring, enabling this will only generate the event. Note: The 'RADIUS Authentication Failure' event type must also be configured in the Event Management view to direct failure events to internal logging and/or external log receivers configured in the Log Receivers view.
Legacy Proxy Configuration	Enable to see the legacy Proxy view. The RADIUS service directly supports the ability to proxy authentication requests and accounting packets to another server by creating a server configuration in the Virtual Servers tab of type 'Proxy'.

Field	Description
	In earlier releases, the FortiNAC server itself would listen for and forward RADIUS packets rather than the RADIUS service. When enabled, this is configured via the 'Legacy Proxy' tab. Devices configured to use Legacy Proxy should be updated to use the new proxy functionality, as the Legacy Proxy is deprecated and will be removed in a future release. Note: Disabling this control will do this automatically using the Virtual Server(s) created during upgrade that match the primary/secondary proxy servers used by Legacy Proxy for that device, as well as monitoring the ports configured in the 'Legacy Proxy' tab for disabled RADS (sic) traffic. If Legacy Proxy Configuration is re-enabled, these devices will need to be manually reconfigured to resume using Legacy Proxy. RELATED INFO: The RFC_Var vendor attribute group is selected by default for devices converted from Legacy Proxy mode, and should be modified manually if this is not the appropriate attribute group for the device.
Security	
RADIUS over TLS (RadSec) Note: Introduced in v7.2.1	Enables a RadSec listener in the RADIUS service that can receive and process secure RadSec communications from devices that support it. The listener is created on the RadSec authentication port. Valid certificates and keys will need to be configured in the System > Certificate Management view for a connection to be established with the client sending authentication request.
Discard Unencrypted Requests	Determines if standard RADIUS packets will still be processed or if only RadSec packets are processed. If this is enabled, a listener will not be created on the authentication port specified in the General Settings section above Security.
Client Certificate Required	When enabled, RadSec communication may only be established when the supplicant provides a valid client certificate. This will require a valid CA Certificate be uploaded in the System > Certificate Management > Trusted Certificates view. When disabled, RadSec communication may be established with only the server certificate being validated.
RadSec Authentication Port	The RADIUS service will listen on for encrypted authentication requests this port. This is typically port 2083.
Ciphers/Protocols	A secure RadSec channel can only be established when the client and server peers both agree on a common cipher and protocol to use. The connection can only be made when the supplicant supports ciphers and protocol versions specified in this section. - Auto Update RadSec Ciphers/Protocols If enabled, the supported RadSec ciphers and TLS protocols will be managed by FortiNAC. - RadSec Protocol(s) If Auto Update RadSec Ciphers/Protocols is disabled, the protocols to user are specified here. - RadSec Cipher(s) If Auto Update RadSec Ciphers/Protocols is disabled, the ciphers to user are

Field	Description
	specified here. Note: If debug is enabled for the RADIUS service, when RadSec is enabled you will see additional listeners indicating FortiNAC is ready to receive and process RadSec requests, noted by the listeners containing "(TLS)":
Require Message-Authenticator	Enabled: Require Message-Authenticator attribute for all Access-Request, Access-Accept, Access-Reject messages to enable BlastRADIUS protection. Disabled: BlastRADIUS protection is disabled. Auto: This is the recommended setting. Enables BlastRADIUS protection for NAS clients that send the Message-Authenticator attribute while still supporting legacy NAS clients that do not. Note BlastRADIUS protection will not be enabled for legacy NAS clients.
Debug & Troubleshooting	Show/hide controls for enabling RADIUS debug. Both RADIUS service and FNAC server debug can be enabled independently. The former is a good starting place for authentication and service startup failures. The latter is useful when authentication succeeds up to the post-auth phase where FNAC does post-auth processing and can diagnose why FNAC returns a deny, incorrect VLAN or filter ID, or wrong/missing response value data (for instance when a device does not have local RADIUS enabled, the port is not in the Role-Based Access port group, etc). • Service Log Level: Enables radius service debug. Debug outputs will be displayed in Service Status > Server Log. ◦ Service Debug Host MAC Filter (Optional): Scope service debug information to one or more (comma separated) host MAC addresses. • FortiNAC Server Log Debug: Enable FortiNAC server debug related to local RADIUS access processing. Debug outputs will be displayed in Service Status > Server Log. ◦ Include Network Access Policy Debug: Include policy lookup debug to troubleshoot problems matching the proper network access policy. For other post-auth issues, leaving this disabled is recommended for better readability. ◦ Service Debug Host MAC Filter (Optional): Scope service debug information to one or more (comma separated) host MAC addresses. Both logs can be used to show both the request attributes and the response attributes for the request. Both MAC filter fields allow the debug to be output only for the specified host MAC addresses. This can be helpful to filter out other requests if troubleshooting is occurring on a production system that is actively processing other requests.

Legacy Proxy



FortiNAC version F 7.4 updated the processing method FortiNAC uses to proxy RADIUS requests. This new enhanced method is referred to as the "Proxy RADIUS Service" and requires a different configuration. Customers configuring Proxy RADIUS for the first time should proceed to [Virtual Servers](#).

Due to this change, the RADIUS Proxy configuration that exists in FortiNAC versions F 7.2 and below is now referred to as "Legacy Proxy". The Legacy Proxy view is available on FortiNAC systems where RADIUS Proxy was configured in a pre-F 7.4 release under **Network > RADIUS > Proxy** and has upgraded to F 7.4 or greater.

Legacy Proxy configurations will continue to work post upgrade.

If the Authentication and Accounting Port settings are not selected (disabled) prior to upgrade, then the Legacy Proxy view will not display once the upgrade is complete. Any saved configurations within this view, however, are preserved. See [Re-Enable Legacy Proxy](#) to re-expose this view.

Customers with Legacy Proxy configurations are encouraged to review the following topics:

- [What's New](#) (Learn about the Proxy RADIUS Service features and enhancements)
- [Convert from Legacy to Virtual Proxy Server](#) (Instructions to start using the Proxy RADIUS Service)

Note: Legacy Proxy configurations are still supported at this time. However, this configuration will be removed in a future release.

Overview

Authentication:

- FortiNAC processes RADIUS MAC but proxies 802.1x EAP authentication to a customer-owned (external) RADIUS server.
- FortiNAC-OS Requirement: "radius-legacy-auth" option must be included in the "set allowaccess" command. See [Open ports](#) for details.

Accounting:

- FortiNAC proxies accounting traffic to a customer-owned (external) RADIUS server.
- FortiNAC-OS Requirement: "radius-legacy-acct" option must be included in the "set allowaccess" command. See [Open ports](#) for details.

FortiNAC works with all the known RADIUS server products, including FortiAuthenticator, FreeRADIUS, Steel Belted RADIUS, Microsoft IAS, Cisco ACS, and RADIATOR. To support these uses, RADIUS server profiles must be created in FortiNAC, which can then be assigned as the authentication method for the FortiNAC system or a specific device.

You can create an unlimited number of RADIUS server profiles. Several configuration options are available:

- System-wide: Default primary and secondary profiles assigned at the system level are used for both captive portal and administrator authentication.
- In an 802.1x environment:
 - Profiles can be assigned for each individual device.
 - Profiles can be assigned for individual SSIDs.

- Profiles can be mapped to domains. User names contain a domain name prefix of the user logging onto the network.
- Profiles can be mapped to a blank domain which would encompass any authenticating user who does not have a domain name prefix as part of his user name.

Fortinet-Group-Name: If the return attributes contain "Fortinet-Group-Name," FortiNAC will create (as needed) a new FNAC group (type user) and add the authenticated user to the group, which can then be used as part of network access policy.

This also applies to cases where FortiNAC is the RADIUS client originating the portal authentication.

When the authentication request is proxied to a proxy RADIUS server and the response is received, the following will occur:

1. Extract group names from attribute "Fortinet-Group-Name"
2. Find the user group for each group name, using "RADIUS" and the proxy server profile name as a prefix. For instance for group "Employee" and proxy server profile "FAC1", consider group "RADIUS/FAC1/Employee"
3. If the user group is not found, create it. Find the user record for the user.
4. If the user record is not found, create it.
5. If the user record is not a member of the user group, add it.
6. Iterate all user groups that exist which start with the "RADIUS + proxy server profile name" prefix but were excluded from the returned Fortinet-Group-Name list and if the user record is found, remove it.

Configuration

RADIUS Proxy port configuration

Allows the RADIUS proxy service to be disabled or the Authentication and Accounting ports to be changed. These ports are independent of each other. This enables FortiNAC to proxy Accounting traffic while processing Authentication requests locally when device models are configured for Local RADIUS Authentication Mode.

RADIUS Server profiles

The first RADIUS Server added becomes the primary server by default. As more servers are added, you can modify which server is the primary.

The encryption method for user names and passwords passed between FortiNAC and the RADIUS server must be set to PAP. This affects the following accounts or user names and passwords created on the RADIUS server:

- The validation account created for communication with FortiNAC and entered in the RADIUS Server Profile configuration.
- Network users that access the network via the captive portal and are authenticated through RADIUS.
- Admin UI users authenticated through RADIUS.
- VPN Users authenticated through RADIUS.

You should be able to communicate with a RADIUS Server in order to add it to the list. For example, if a RADIUS Server is not currently connected to the network and FortiNAC cannot contact it, you will be asked if you want to add the server anyway.

1. Click **Network > RADIUS**
2. Click **Proxy** from the upper right hand corner.

Configure Proxy service

1. Modify the following as appropriate:
 - **Authentication Port:** Enables/disables the service and defines the authentication port for the RADIUS Proxy.
Default: Enabled, 1812 (Cannot be set to the same port as Local RADIUS Authentication port)
 - **Accounting Port:** Enables/disables the service and defines the accounting port for the RADIUS Proxy.
Default: Enabled, 1813
2. Click Save Settings. Changes to the configuration apply within 0-30 seconds.

Add a profile

1. Click **Add**.
2. Enter the parameters for the RADIUS Server profile.
3. Click the **RADIUS Secret** field to enter the RADIUS secret.
4. Enter the User Name.
5. Click the **Password** field to enter the Password information.

Field	Definition
Profile Name	Name displayed in the RADIUS server list.
Host Name/IP address	Host name or IP address of the RADIUS server. If you are generating certificates using a NSRADIUS appliance, the Fully Qualified Domain Name is required.
RADIUS Secret	Encryption key used by the RADIUS server to send authentication information.
Authentication Port	Port number through which the RADIUS server communicates.
Accounting Port	Port number that the RADIUS server uses for the accounting features, if they are used. If your RADIUS server does not use accounting features, leave the check box blank.
Last Modified By	User name of the last user to modify the RADIUS Server.
Last Modified Date	Date and time of the last modification to this RADIUS Server.
Validation account	
User Name	User name for verifying access to the RADIUS Server. This field is required, but only used when there are multiple RADIUS Servers configured. You must create an account on the RADIUS Server that is used by FortiNAC to communicate with that Server. The encryption method must be set to PAP.
Password	Password for verifying access to the RADIUS server. This field is required.

6. New servers are saved automatically.
7. Repeat as needed for additional RADIUS servers.

Modify a profile

1. Click **Network > RADIUS > Proxy**
2. Select the RADIUS Server profile and click **Modify**.
3. Make the changes. Changes are saved automatically.

Delete a profile

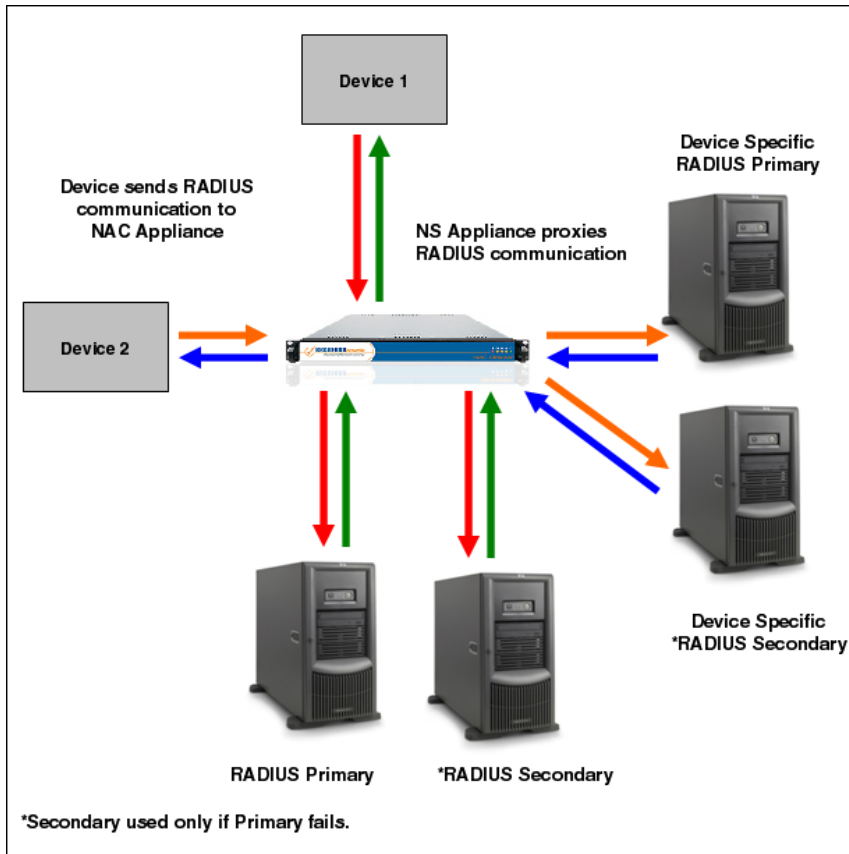
1. Click **Network > RADIUS > Proxy**
2. Select the RADIUS Server profile and click **Delete**.

Failover process

In FortiNAC you can have primary and secondary RADIUS servers that are the system-wide default for RADIUS requests. You can also have other RADIUS servers that are listed as the primary and secondary server for requests coming through a specific device.

All of these RADIUS servers must be configured in FortiNAC and must be running in parallel. It is required that each RADIUS server be configured with a user name and password that will be used by FortiNAC as a Validation Account to test for RADIUS server availability. That user name and password must also be entered into the RADIUS server configuration within FortiNAC allowing a test message to be sent to the RADIUS server.

If one or both of your RADIUS servers were to fail, there is a failover process that is followed. No events or alarms are generated when a RADIUS server fails. There are two types of failure in this process. The first is a failure by the RADIUS server to respond to a RADIUS communication sent from a device and proxied by FortiNAC. This does not indicate that the RADIUS server is not running, simply that it did not accept or respond to the communication. The second type is a failure caused because the RADIUS server is down and FortiNAC cannot communicate with it.



Failover

1. FortiNAC receives a RADIUS communication.
2. The RADIUS communication is proxied to the configured primary RADIUS server.
3. The primary server responds.
4. If the primary server does not respond, the original RADIUS communication is not processed nor is any response sent to the device. FortiNAC contacts the primary RADIUS server with the validation account to validate RADIUS communication.
5. If the primary server responds to FortiNAC, then the primary RADIUS server continues to be used for subsequent incoming RADIUS communications.
6. If the primary server does not respond to FortiNAC, FortiNAC begins sending new RADIUS communications to the secondary RADIUS server.
7. The secondary server responds.
8. If the secondary server does not respond, the RADIUS communication in progress is not processed nor is any response sent to the device. FortiNAC contacts the secondary RADIUS server with the validation account to validate RADIUS communication.
9. If the secondary server responds to FortiNAC, then it continues to be used for subsequent RADIUS communications until contact is re-established with the primary server.

Recovery

1. If the primary server fails FortiNAC continues to attempt to communicate with the primary RADIUS server at six second intervals. This setting is not configurable.
2. The secondary server continues to be used until a response is received from the primary RADIUS server. The primary server is used for subsequent RADIUS communications.
3. If both the primary and the secondary servers have failed, FortiNAC continuously attempts to contact both the primary and the secondary RADIUS servers at six second intervals. The primary server is considered to be "in charge" at that point even though neither server is responding.
4. As soon as either RADIUS server responds, FortiNAC begins sending RADIUS communications to that server.
5. If it is the secondary server that responded, FortiNAC continues trying to contact the primary server. When the primary server responds, it is used for subsequent RADIUS communications.
6. If it is the primary server that responded, FortiNAC uses the primary server for subsequent RADIUS communications.

Validate redundant RADIUS

Validate that your redundant RADIUS servers are functioning properly. That is, when the primary RADIUS server fails, control passes successfully to the secondary, which then continues handling authentication messages until control can successfully be returned to the primary RADIUS server.

To test redundancy, keep the following details in mind:

- The RADIUS server is actually a service running on a server.
- Primary and secondary RADIUS servers run on separate servers (computers) not on the FortiNAC appliance.
- For this test RADIUS requests are generated by logging in a host through the Captive Portal.

Test setup

1. Log in to the CLI on your FortiNAC appliance and enable debug by typing `campusmgrdebug -name RadiusManager true`.
2. Make sure both RADIUS servers are up and running, so communication is proxied to the primary.
3. Monitor the output.master file in the `/bsc/campusMgr/master_loader` directory on the FortiNAC Control Server for the RADIUS messages that are generated by this test.

Force a failover

1. Turn off the primary RADIUS service.
2. Send a RADIUS request (use a computer to log in through the portal).
3. Verify that the primary RADIUS server fails to respond. You will see that it retries, and finally times out.
4. Verify that a RADIUS request is initiated using the Validation Account (specified in the RADIUS configuration in the admin UI for the FortiNAC appliance) and that this also fails. You should see a message in the output.master file similar to "Contact Message being sent".
5. Verify that the primary RADIUS server is added to the Failover list - you can read that FortiNAC is adding the primary RADIUS server to the list, and when a new request comes in you will see that FortiNAC checks this list by reading the output.
6. Confirm that requests are sent repeatedly to the primary RADIUS server to see if it is up and running (e.g., every 5 - 6 seconds).

-
7. Send a RADIUS request by logging in through the portal again.
 8. Confirm that the secondary RADIUS server responds correctly.

Restore the primary server

1. Turn the primary RADIUS service back on.
2. Send a RADIUS request by logging in through the portal.
3. Confirm that the primary RADIUS server responds correctly.

Disable both servers, then restore the primary

1. Turn off both RADIUS services.
2. Send a RADIUS request by logging in through the portal.
3. Verify that requests are sent repeatedly to both the primary and secondary RADIUS servers.
4. Turn on the primary RADIUS server.
5. Send a RADIUS request by logging in through the portal.
6. Confirm that the primary RADIUS server responds correctly.

Disable both servers, then restore the secondary

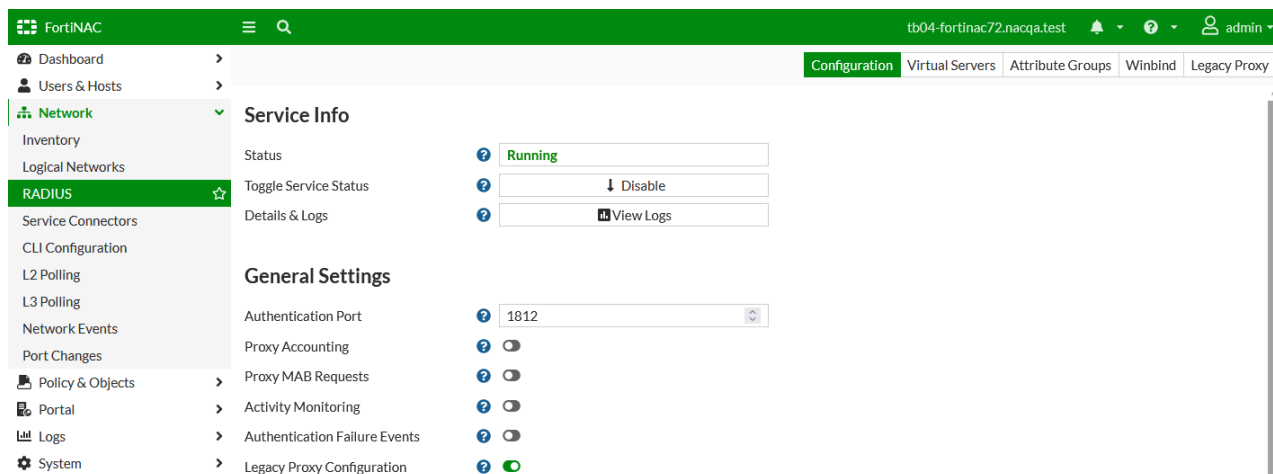
1. Turn off both RADIUS services.
2. Turn on the secondary RADIUS server.
3. Send a RADIUS request by logging in through the portal.
4. Confirm that the secondary RADIUS server responds correctly.

Upgrade Procedure (Existing Proxy Configurations)

The RADIUS Proxy functionality that exists in FortiNAC versions 7.3 and below is deprecated as of version 7.4. This functionality was configured under **Network > RADIUS > Proxy** and is now referred to as "Legacy Proxy".

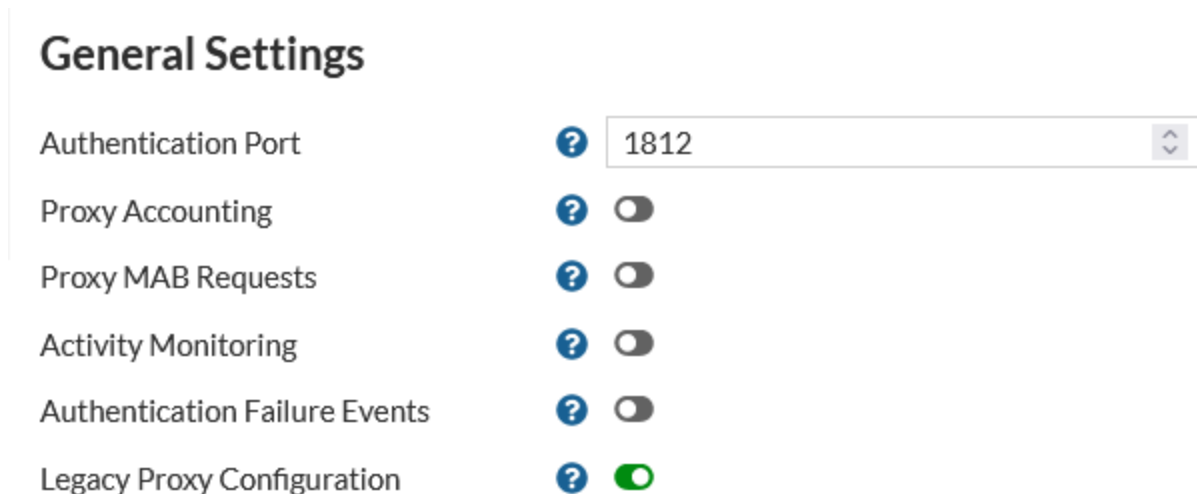
The steps below allow customers to familiarize themselves with the new views and confirm the proxy functionality post upgrade. Assumes customer has RADIUS proxy already configured and running in a version prior to 7.4.

1. Upgrade to 7.4 or greater.
2. Clear browser cache and login to the FortiNAC UI.
3. Navigate to **Network > RADIUS**.
4. **Virtual Servers** and **Legacy Proxy** tabs should now display.



New Virtual Proxy Servers are automatically created during upgrade under the **Virtual Servers** tab. These virtual servers should match the legacy server configurations.

5. If the **Legacy Proxy** tab is not visible, enable the **Legacy Proxy Configuration** under **General Settings**. If this option is not listed, proceed to **Re-Enable Legacy Proxy**.



6. Click **Legacy Proxy** to review the RADIUS Proxy settings previously configured under **Network > RADIUS > Proxy**.

FortiNAC 23 seconds until session expires tb04-fortinac72.nacqa.test admin

Configuration Virtual Servers Attribute Groups Winbind **Legacy Proxy**

Add Modify Delete Validate

RADIUS Proxy Port Configuration

Warning: Legacy RADIUS Proxy functionality is deprecated and will be removed in a future release. The configuration below uses the FortiNAC server to listen for and proxy authentication requests. RADIUS proxying is now natively supported by the RADIUS service by creating Virtual Servers of type Proxy. New Virtual Proxy Servers have been automatically created during upgrade to match the legacy primary/secondary server configurations in use by devices in the topology that have RADIUS Mode set to Legacy Proxy. These Virtual Servers should be validated for accuracy, and all devices/VDOMs/SSIDs configured to use the Legacy Proxy should be modified, changing 'RADIUS Mode' from 'Legacy Proxy' to 'RADIUS Service'. For convenience, multiple devices/VDOMs/SSIDs may be selected and configured together by selecting 'Set Model Configuration' or 'SSID Configuration' from the right click menu. Once all devices are using the new proxy functionality, legacy proxy functionality can be disabled entirely by disabling 'Legacy Proxy Configuration' in the RADIUS Configuration tab.

☐ Authentication Port 1812

☐ Accounting Port 1813

RADIUS Servers - Total: 1

Profile Name	Host Name/IP	Authentication Port	Accounting Port	User Name	Last
LegacyProxy	10.106.90.30	1812	1813	radius1	admin

7. Under the device's Model Configuration, click **Legacy Proxy** to review the settings.

Confirm

Domain Configuration

SSO Addresses ? SSOGRP:FGVM04TM23010645:root

VPN Addresses ? VPNGRP:FGVM04TM23010645:root

RADIUS Mode ? RADIUS Service **Legacy Proxy**

RADIUS

RADIUS Secret ? Change

Source IP Address ? 192.168.2.1

Primary RADIUS Server ? LegacyProxy

Secondary RADIUS Server ?

FortiNAC will continue to function as before. Customers using the Legacy Proxy functionality are advised to move to the new Proxy RADIUS Service before the Legacy Proxy feature is removed in a future FortiNAC release.

Re-Enable Legacy Proxy

If the Authentication and Accounting Port settings are not selected (disabled) prior to upgrade, then the Legacy Proxy view will not display once the upgrade is complete. Any saved configurations within this view, however, are preserved.

If the Legacy Proxy views do not display upon upgrade, re-expose and re-enable the legacy functionality using the FortiNAC CLI.

1. Login to the CLI and type the below commands.

```
execute enter-shell
globaloptiontool -name "radiusServer.legacyProxySupported" -set true
globaloptiontool -name "radiusServer.legacyProxyUIEnabled" -set true
exit
exit
```

2. The **Legacy Proxy** tab should be visible and contain the RADIUS server profile. Review settings to ensure accuracy.

The screenshot shows the FortiNAC web interface with the 'Legacy Proxy' tab selected. The interface includes a sidebar with navigation options like Dashboard, Users & Hosts, Network, RADIUS, and Policy & Objects. The main content area displays the 'RADIUS Proxy Port Configuration' section with a warning message and checkboxes for 'Authentication Port' (1812) and 'Accounting Port' (1813). Below this is a table titled 'RADIUS Servers - Total: 1' with columns for Profile Name, Host Name/IP, Authentication Port, Accounting Port, User Name, and Last. The table contains one entry for 'LegacyProxy' with Host Name/IP '10.106.90.30', Authentication Port '1812', Accounting Port '1813', User Name 'radius1', and Last 'admin'.

Profile Name	Host Name/IP	Authentication Port	Accounting Port	User Name	Last
LegacyProxy	10.106.90.30	1812	1813	radius1	admin

3. Select the RADIUS Mode **Legacy Proxy** and review the device's Model Configuration.

FortiNAC will continue to function as before. Customers using the Legacy Proxy functionality are advised to move to the new Proxy RADIUS Service before the Legacy Proxy feature is deprecated in the future. For instructions, see [Convert from Legacy to Virtual Proxy Server](#).

Convert from Legacy to Virtual Proxy Server

This process assumes FortiNAC is running version 7.4.0 or greater and **Network > RADIUS > Legacy Proxy** is configured and in use.

1. Go to **Network > RADIUS > Virtual Servers**

2. Validate the new Virtual Proxy Server configurations for accuracy.

If one was not created automatically during upgrade, select **Create New** and fill in the following fields:

- Name: Name of the configuration defining the connection between a proxy RADIUS server and FortiNAC
- Type: Select **Proxy**
- Proxy Servers: Click + and select the proxy server from the menu. Then click **Close**.

3. Click **OK** to save. The new Virtual Proxy Server should now display in the **Virtual Servers** table.

4. Go to **Network > Inventory**.

5. Modify the RADIUS mode on all devices/VDOMs/SSIDs configured to use the Legacy Proxy.

Option 1: Modify individually (Model Configuration/SSID configuration)

- a. Select the device in Inventory and select **Model Configuration** or **SSID Configuration**.
- b. Select **RADIUS Service**.
- c. In the **Server Configuration** drill-down menu, select the new Virtual Proxy Server.
- d. The RFC_Vlan default attribute group is selected by default for devices converted from Legacy Proxy mode. It should be modified manually if this is not the appropriate attribute group for the device. See [Attribute Groups](#) for details.
- e. Select **OK** to save.

Validate functionality.

a. Option 2: Modify multiple (Set Model Configuration)

For convenience, multiple devices/VDOMs/SSIDs may be selected and configured together by selecting “Set Model Configuration” or “SSID Configuration” from the right click menu.

- i. Under the Devices/SSID/Virtualized Devices tab in Inventory, multi-select the right click and select **Set Model Configuration**.
- ii. From drill-down menu, select **Detail Configuration**.
- iii. Select **Enable RADIUS** and select **RADIUS Service**.
- iv. Select **Server Configuration** and select the new Virtual Proxy Server from the drill-down.
- v. The RFC_Vlan default attribute group is selected by default for devices converted from Legacy Proxy mode. It should be modified manually if this is not the appropriate attribute group for the device. See [Attribute Groups](#) for details.
- vi. Select **OK** to save.
- vii. Validate functionality.

6. Once all devices are using the new proxy functionality, disable the “Legacy Proxy Configuration” under **Network > RADIUS > Configuration**.

Virtual Servers

Used to display and modify RADIUS server configurations. There are two types of virtual servers: Local and Proxy.

The following table provides basic information regarding both server types.

Function	Local Server Type	Proxy Server Type	Required “set allowaccess” Option (FortiNAC-OS)
Authentication	Processes RADIUS MAC and 802.1x EAP authentication without the need to proxy to an external RADIUS server. Supported 802.1x EAP modes: • TLS • TTLS/MSCHAPv2 • TTLS/PAP • PEAP/MSCHAPv2 • TEAP • MD5 • GTC • MSCHAPv2 • FAST	Processes RADIUS MAC but proxies 802.1x EAP authentication to a customer-owned external) RADIUS server.	Local & Proxy Server: <code>radius-auth</code> Legacy Proxy Server: <code>radius-legacy-auth</code> See Open ports for details.
Accounting	The Local Server does not provide accounting. If accounting is required, FortiNAC can be configured to proxy Accounting traffic to an external RADIUS server.	Proxies accounting traffic to a customer-owned (external) RADIUS server. In some RADIUS integrations, FortiNAC can also process these packets. Refer to the integration guides in the Document Library for details.	Local & Proxy Server: <code>radius-acct</code> Legacy Proxy Server: <code>radius-legacy-acct</code> See Open ports for details.
RadSec	Processes RADIUS over TLS (RadSec) requests from clients that support it. See Configure Local RADIUS Server settings for details.	N/A	<code>radius-radsec</code>

Add/Modify a Virtual Server

1. Navigate to **Network > RADIUS**.
2. Click **Virtual Servers**.
The virtual server DefaultConfig is already created and can be configured as desired.
3. Modify the existing virtual server by highlighting it and selecting **Edit**. Otherwise select **Create New**.
4. Configure a **Name** for the virtual sserver configuration.
5. Select the **Type** from the drop down menu:
Local: Authentication requests from devices using this virtual server configuration will be processed locally. If selecting this type, see [Configure Local Server](#).
Proxy: Authentication requests from devices using this virtual server configuration will be proxied to an external RADIUS server. If selecting this type, see [Configure Proxy Server](#).

Delete a Virtual Server

1. Select the server and click **Delete**.
2. The user is prompted to select a replacement RADIUS server configuration to use for RADIUS enabled devices that were using the deleted server(s).
The new configuration will also be used for FLR designated proxy servers supporting Euduroam IdP functionality if applicable.
If **None** is specified, authentication requests from those devices will not be processed until a server configuration is set.

Configure Local Server

Configure the Local server using the table below. Click **OK** to save.

Field	Definition
TLS Configuration	TLS Certificate, protocols, and cipher suites to use for EAP-TLS negotiation. Can either select the default RADIUS EAP configuration, or create a new one. New TLS Service Configuration Click (+) and configure the following then click OK to save (See tooltips in the UI next to each selection): • Name • Certificate Alias • Auto Update Ciphers/Protocols (On/off) If Auto update is disabled, configure the following: • TLS Protocol(s) supported for TLS negotiation • TLS 1.3 • TLS 1.2 • TLS 1.1 (Not Recommended) • TLS 1.0 (Not Recommended)

Field	Definition								
	• Cipher suites for encrypting EAP-TLS tunnels. Click on each option in list to add.								
Supported EAP Types	EAP Types enabled for this server configuration. Available options are: TLS TTLS PEAP MD5 GTC MSCHAPV2 FAST TEAP								
Winbind Domain(s)	For MSCHAPv2 authentication, specify the winbind instances for the allowed Active Directory Server(s) or 'Allow Any' for authentication using any defined servers. Manage winbind instances in the Winbind tab.								
OCSP Enabled	Enable Online Certificate Status Protocol support, which checks for revocation status of certificate in real time. For references on setting up a OCSP responder for Certificate Authority (CA), please see Microsoft Certificate Services Configuring OCSP.								
Timeout	The amount of time sets for OSCP responder to respond with the certificate status.								
OCSP Soft Fail	When enabled, FortiNAC RADIUS server checks for network errors such as timeout, DNS failure, and unreachable OCSP responder before failing the certificate. It is useful when the OCSP responder is located in a unreliable network environment. These are 3 scenarios with OCSP Soft Fail: <table> <tr> <th>OCSP validation with OSCP Soft Fail Enabled</th><th>Authentication Result</th></tr> <tr> <td>When the certificate is valid and FortiNAC RADIUS server can retrieve certificate status from the OCSP responder.</td><td>Pass</td></tr> <tr> <td>When the certificate is expired and FortiNAC RADIUS server can retrieve certificate status from the OCSP responder.</td><td>Fail</td></tr> <tr> <td>When the certificate is valid and FortiNAC RADIUS server cannot retrieve certificate status from the OCSP responder within the time-out range.</td><td>Pass</td></tr> </table>	OCSP validation with OSCP Soft Fail Enabled	Authentication Result	When the certificate is valid and FortiNAC RADIUS server can retrieve certificate status from the OCSP responder.	Pass	When the certificate is expired and FortiNAC RADIUS server can retrieve certificate status from the OCSP responder.	Fail	When the certificate is valid and FortiNAC RADIUS server cannot retrieve certificate status from the OCSP responder within the time-out range.	Pass
OCSP validation with OSCP Soft Fail Enabled	Authentication Result								
When the certificate is valid and FortiNAC RADIUS server can retrieve certificate status from the OCSP responder.	Pass								
When the certificate is expired and FortiNAC RADIUS server can retrieve certificate status from the OCSP responder.	Fail								
When the certificate is valid and FortiNAC RADIUS server cannot retrieve certificate status from the OCSP responder within the time-out range.	Pass								
Authentication Source	The Microsoft Entra ID application which is the identify source that performs the user authentication.								

Field	Definition
Client Certificate Attribute	Note: F 7.6.3+ only Enable to retrieve the host name through the specific RADIUS attribute. If the user would like to retrieve hostname from the filed UPN, Client Certificate Attribute must be enabled, and the client configured with user principal name manually. For both machine and user authentication, FortiNAC supports retrieving hostname from CN, DNS, UPN. The ranking table enables you to prioritize client certificate attributes by arranging them in order of preference. Simply drag and drop the attributes to set the desired order, which determines which attribute will be retrieved first when accessing user information from the certificate. The default client certificate ranking is Common Name (CN), SAN (Subject Alternative Name)-UPN, SAN-DNS, and SAN-EMAIL. If Client Certificate Attribute is disabled, the user needs to have the correct Common Name in their client certificate.
Allow Spaces in User Name	Enable to allow client certificate common name (CN) or subject alternative name (SAN) to have white spaces.
TEAP/FAST PAC Settings	TEAP (Tunnel Extensible Authentication Protocol) is a tunnel-based Extensible Authentication Protocol method that establishes a secure tunnel and executes other EAP methods under the protection of that secured tunnel. TEAP authentication occurs in two phases after the initial EAP identity request/response exchange. In the first phase, TEAP uses the TLS handshake to provide an authenticated key exchange and to establish a protected tunnel. Once the tunnel is established, the second phase begins with the peer and the server engaging in further conversation to establish the required authentications and authorization policies. Note: F 7.6.3+ only Primary Auth Type: Primary authentication method used during TEAP authentication. EAP-MSCHAPv2 and EAP-TLS are supported for TEAP inner methods. Value options are User or Computer. Secondary Auth Type: Optional secondary authentication method used during TEAP authentication. EAP-MSCHAPv2 and EAP-TLS are supported for TEAP inner methods. Value options are User or Computer.
PAC Opaque Key	The PAC opaque key is a secret cryptographic value used to encrypt and validate the Protected Access Credentials (PACs). This key ensures that the PAC data remains confidential and tamper-proof throughout the authentication process. A PAC (Protected Access Credential) is a credential issued to a client during a successful full TEAP/FAST authentication (must be exactly 32 bytes in size) that contains cryptographic keys and session parameters needed for fast, secure session resumption. The opaque key is used to encrypt and validate this PAC, ensuring that the credential remains confidential and tamper-proof, which in turn enables abbreviated reauthentication without repeating the entire TLS handshake.
Allow Anonymous In-Band PAC Provisioning	TEAP/FAST authentication uses (in addition to TLS Configuration ciphers): Anonymous Diffie-Hellman ciphersuites (ADH).

Field	Definition
Allow Authenticated In-Band PAC Provisioning	TEAP/FAST authentication uses (In addition to TLS Configuration ciphers): TLS_RSA_WITH_RC4_128_SHA, TLS_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TEAP configuration

TEAP (Tunnel Extensible Authentication Protocol) is a tunnel-based Extensible Authentication Protocol method that establishes a secure tunnel and executes other EAP methods under the protection of that secured tunnel.

TEAP authentication occurs in two phases after the initial EAP identity request/response exchange. In the first phase, TEAP uses the TLS handshake to provide an authenticated key exchange and to establish a protected tunnel. Once the tunnel is established, the second phase begins with the peer and the server engaging in further conversation to establish the required authentications and authorization policies.

Procedure

Step 1: Update Local RADIUS Server Certificate

1. Navigate to **System > Certificate Management**.
2. Generate a CSR. Enter the cert information.
3. Sign the CSR using OpenSSL with the following command:

```
openssl x509 -req -copy_extensions copyall -days 3650 -in TEAP.csr -CA ca.crt -CAkey ca.key
-CACreateserial -out server.crt -sha256 -extensions req_ext -extfile <(printf "[req_ext]\nextendedKeyUsage=serverAuth,clientAuth")
```
4. Verify the EKU field:

```
-CA- openssl x509 -in server.crt -text -nooutls -
```
5. Upload the signed certificate to the RADIUS server as the EAP certificate.

Step 2. Configure RADIUS Server

1. Go to **Network > RADIUS > Virtual Servers**.
2. Select the appropriate virtual server and enable **TEAP**.
3. Ensure Windows AD is connected under **Network > RADIUS > Winbind**.

Step 3. Enable Dot1X

1. Go to **Network > Inventory**. Select the FortiSwitch.
2. Right-click the port where the client is connected.
3. Select **Port Properties** and check Dot1x auto registration.
4. On FortiGate: Navigate to **WiFi & Switch Controller > FortiSwitch Ports** and apply the 802.1X security policy on the port.

Step 4. Configure Network Access Policy

1. Navigate to **Policy & Objects > Network Access**.
2. Create a new policy.
3. Follow on-screen setup instructions.

Validate

1. On the client machine, navigate to **Network Adapter Properties > Authentication**.
2. Select EAP TEAP as the authentication method
3. Click **Settings**, and:
Select the appropriate Trusted Root Certification Authority.
Choose **EAP-MSCHAPv2** under Client Authentication.
Enter user credentials from LDAP.
4. Verify the following:
 - Client receives IP address from production VLAN (e.g., VLAN 10).
 - Check RADIUS logs for authentication errors.

Configure Proxy Server

Define one or more proxy RADIUS servers that will service authentication requests for devices using this configuration.

NOTE: If domain mappings are configured and a user's domain matches a mapping, the request will be forwarded to the server in the mapping, regardless of the server's specified in this list.

Proxy servers can be deleted from the **Network > Service Connectors** view once removed from all virtual servers and domain mappings.

1. Click **+** next to **Proxy Servers**.
2. Click **+ Create**.
3. Configure the RADIUS server profile using the table below. Click **OK** to save.

Field	Definition
Profile Name	Name of the configuration defining the connection between a proxy RADIUS servers and FortiNAC.
Host Name/IP Address	Host name or IP address of the RADIUS server.
RADIUS Secret	Encryption key used by the RADIUS server to send authentication information.
Server Type	Specify the type of requests processed by the server: Authentication Authentication & Accounting
Port	Authentication port This value can either be typed in or use the up and down arrows. Note: When Server Type is set to both Authentication & Accounting, the specified port is the authentication port, and the accounting port will be (authentication port +1).
Eduroam FLR	No – Not using Eduroam Eduroam enabled networks only – Servers designated as a Federation Level RADIUS server (FLR) will be used to authenticate roaming guests on this network against that user's Eduroam Identity Provider (IdP).

A secondary is used for failover when the primary becomes unreachable, or for load-balancing.

When Eduroam IdP functionality is enabled for this network, FLR designated servers will be registered as a valid source of RADIUS authentication requests so local users roaming on other Eduroam Service Providers (SP) can authenticate back to this network acting in an IdP capacity via the FLR. Setting to Primary or Secondary will replace any other server with that designation.

To enable IdP capability, an Eduroam IdP Server Configuration must be set in the **Roaming Guests settings** view.

Note: Enable Eduroam SP capability by configuring local domains in the Roaming Guests settings view, or by creating a dedicated eduroam virtual server that proxies to the FLRs, and setting it as the RADIUS server configuration on a dedicated eduroam SSID.

See [Eduroam Cookbook](#) for details.

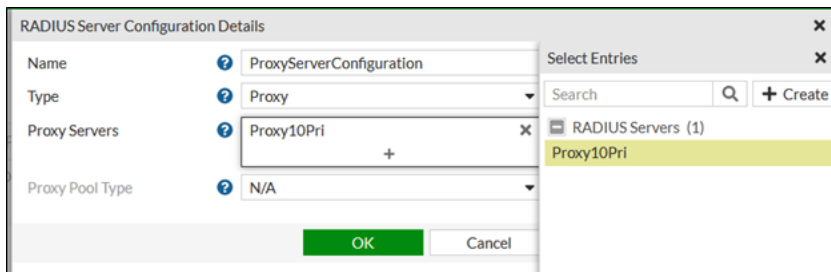
Portal/Admin Default Server
(Enable/Disable)

For portal and admin login using RADIUS authentication.

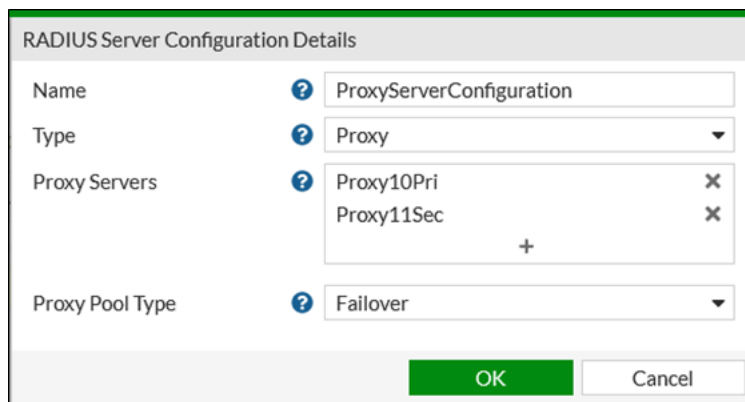
Use this server unless the user's domain matches a configured RADIUS domain mapping.

Enabling will replace the previous default if one is configured. This information can also be seen and configured in the **Network > RADIUS > Virtual Servers > DomainMappings** table.

- Click on the new server profile to add to the Proxy server configuration. The server will populate the **Proxy Servers** field. **Note:** Once created, the server can be viewed and modified under **Network > Service Connectors**.



- Select or create another Proxy server to add to the Proxy servers field or click **Close**.
Note: If using multiple Proxy servers and the intent is for them to be used in a failover configuration, add the server acting as the primary to the list first, then the secondary.
- If multiple proxy servers are selected, set the **Proxy Pool Type**:
Failover: The first server in the specified order is used unless it is down. In which case, the second is used and so on.
Load Balance: Requests are split evenly among all specified servers.



RADIUS Server Configuration Details

Name: ProxyServerConfiguration

Type: Proxy

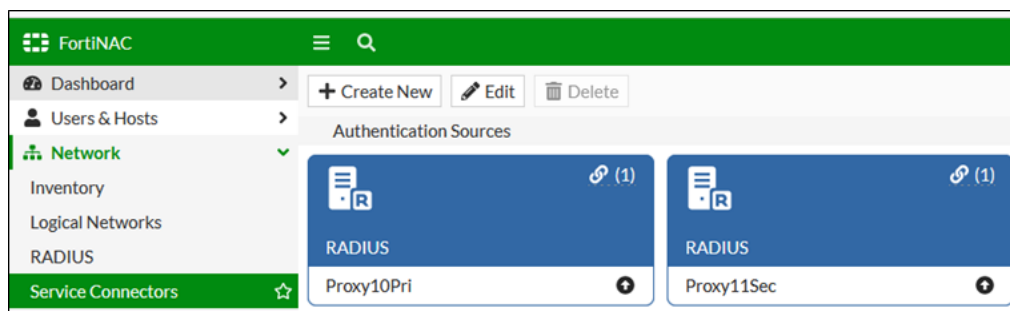
Proxy Servers: Proxy10Pri, Proxy11Sec

Proxy Pool Type: Failover

OK Cancel

7. Click **OK** to save.

The Proxy servers will now display as RADIUS Service Connectors under **Network > Service Connectors**.



Remove Proxy Server from the Server Configuration

1. Double click on the Virtual Server or highlight and click **Edit**.
2. Click on the **Proxy Servers** field.
3. In the right panel under **RADIUS Servers**, click on the server to remove it from the **Proxy Servers** field.
4. Click **Close**.
5. Click **OK** the save.

Domain Mappings

Optional. Use domain mappings to determine which RADIUS server to use for authentication.

If the domain prefix contained within the user name of a connecting user matches a mapping, then the RADIUS server mapped to that domain is used.

Multiple servers can be mapped to a single domain. If the user is not found on the first RADIUS server in the list (starting at Rank 1), FortiNAC checks each server mapped to the domain in turn until the user is found.

For more on Order of precedence, see [RADIUS](#).

Add a Domain Mapping

1. Navigate to **Network > RADIUS**.
2. Click **Virtual Servers**.
3. Under the **Domain Mappings** panel, click **Create New**.
4. Configure using the table below.

Domain Mapping Details

Field	Definition
Domain	When the user domain in the incoming request matches this value, the specified Proxy Server will be used for the request.
Portal/Admin Default	For portal and admin login using RADIUS authentication: Use the specified server for all authentication requests unless the user's domain matches another domain mapping.
Proxy Server	The proxy server that will process the authentication request when the user's domain matches this mapping's domain. Select the server using the drop down menu. If the server is not yet created, click Create and configure the RADIUS server profile. See Configure Proxy Server for details.

5. Click **OK** to save.

Mappings can be ranked using the **Rank Up** and **Rank Down** buttons.

Attribute Groups

Allows administrators to control the RADIUS attributes the FortiNAC Local RADIUS Service returns in Access-Accept, Disconnect-Request and CoA-Request packets

- Build groups from a large collection of known RADIUS attributes, both standard and vendor-specific. Custom attributes can also be created.
- Can be configured at device level and logical network level scope for both simple and complex deployments
- Returned attributes are a combination of device and logical network level groups. The more granular logical network attributes take precedence
- Each of these attributes can be optionally scoped so debug output is only generated for 1 or more specified MAC addresses (comma separated).

Requirements

- Device models using these groups must be configured for Local RADIUS Authentication mode.
- Inbound RADIUS request must contain Calling-Station-Id. This attribute is required in order to properly process logical network information. RADIUS attributes will not be returned if Calling-Station-Id is not in the associated request. **Note:** The Calling-Station-Id attribute is also required for custom Disconnect Message and CoA Message attribute groups.

RADIUS Attribute Groups are configured in the RADIUS Attribute Groups view. Once the Attribute Groups are defined, they can be deployed to the network via Model Configuration and SSID configuration views.

Add RADIUS Attribute Group

1. Navigate to **Network > RADIUS**.
2. Click **Attribute Groups**.
3. Click **Add**.
4. Use the filter to narrow down the list of attributes in the left pane, and select them by clicking the arrow icons to push them into the right pane.
5. Set the value by clicking the value box on the right pane.
6. Setting to %ACCESS_VALUE% will insert the Access Value into the attribute when returned.

%AUTH%	The attribute to be used in the Disconnect or CoA request should be copied from the Authentication request.
%ACCT%	The attribute to be used in the Disconnect or CoA request should be copied from a related accounting request.
%ACCESS_VALUE%	The Access Value (VLAN or Policy value).
%System%	The attribute to be used in the message is coming from system, system fills them in as appropriate

Add Custom RADIUS Attribute

If the attribute required does not exist in FortiNAC's database, it can be added.

Note: RADIUS Attribute Response Value character limit is 253.

1. In **Add RADIUS Attribute Group**, click **Add**, then **Add Custom RADIUS Attribute** will pop-up.
2. Define the following:
 - Name
 - Type: Select the appropriate option from the drill-down list.
 - Value
 - Vendor
 - Vendor ID
 - Format
 - Has Tag:
 - Encryption method: Select the appropriate option from the drill-down list.
3. Click **OK** to save.
4. To modify an attribute added, click **Modify**. **Note:** Pre-loaded attributes may not be edited.
5. To delete an attribute, select **Delete**.

Once the Attribute Groups are defined, they can be applied in a number of ways:

- Assign a Default RADIUS Attribute Group
 - Per Individual Device Model See [Model configuration](#).
 - Multiple Device Models simultaneously – See [Deploy Attribute Groups in Bulk – Model Configuration](#).
 - Per SSID - See [SSID configuration](#).
 - Multiple SSIDs simultaneously - See [Modify multiple SSIDs](#).
- Assign an Additional RADIUS Attribute Group per Logical Network – See [Model configuration](#).

Deploy Attribute Groups in Bulk – Model Configuration

Note The values set through this method may not apply to all selected devices equally. For example, four devices are selected, but only two devices have the Logical Network “Aruba” configured. Any modifications made in this view for the “Aruba” Logical Network will only apply to those devices with “Aruba” configured.

1. Click Network > Inventory
2. Select the container where the devices are located.
3. In the Devices view, use Ctrl-click or Shift-click to select the devices to modify.
4. Right-click the devices and click **Set Model Configuration**.

Apply Default Attribute Group

1. From the top drill down menu, select **Detail Configuration**.
2. Click the **Enable RADIUS** checkbox.
3. Click **Enable Local**.
4. Click the **Default RADIUS Attribute Group** checkbox. The associated drill down menu will appear.
5. From the drill down, select the desired **RADIUS Attribute Group**.
6. Click **OK** to save changes or proceed to define additional **RADIUS Attribute Groups**.

Apply Additional RADIUS Attribute Groups to Logical Networks

1. From the top drill down, select the desired **Logical Network** to modify.
2. Click **Additional Attribute Group** checkbox. The associated drill down menu will appear.
3. From the drill down, select the desired **RADIUS Attribute Group**.
4. Repeat steps 10-12 to add and modify additional **Logical Networks** as needed.
5. Click **OK** to save changes.

Configure RFC 5176 message type and RFC5176 Attribute Groups

1. From the top drill down, select the desired Logical Network to modify.
2. Enable **Access Enforcement** and select **Enforce**.
3. Enable **RFC5176 Message Type** and **RFC5176 Attribute Groups**.
4. For details, see RFC5176 Message Type and RFC5176 Attribute Group in [Model Configuration](#).
5. Click **OK** to save changes.

For additional details on this feature as well as configuration examples see [RFC5176 CoA/Disconnect Message](#) in the Document Library.

Applying Dynamic Access Control List (DACL)

Attribute Groups can be configured to apply DACLs. Refer to the following articles for configuration examples:

FortiSwitch (FortiLink Mode): <https://community.fortinet.com/t5/FortiNAC-F/Technical-Tip-CoA-Support-in-FortiNAC-7-4-and-applying-DACLs-in/ta-p/322638>

Cisco Switches: <https://community.fortinet.com/t5/FortiNAC-F/Technical-Tip-How-to-send-Downloadable-ACL-DACL-to-Cisco-Switch/ta-p/395698>

Winbind

Winbind is used to provide MSCHAPv2 authentication only. If using a different scheme, such as EAP-TTLS/PAP or EAP-TLS, configuration is not required.

Note: FortiNAC is unable to encrypt Winbind connections with LDAPs or starttls.

Multiple Winbind instances can be created.

1. Navigate to **Network > RADIUS > Winbind** to configure winbind settings.
2. Service information can be edited from the main Winbind view while **Winbind Domain Configuration Details** can be configured by creating or selecting an existing winbind and selecting Edit.
3. Configure using the table below.

Service Info

Field	Description
Toggle Service Status	Enable/Disable processing of MSCHAPv2 authentication requests Note: FortiNAC must be joined to the domain before starting the Winbind service.
Status	• Enabled Status: Displays ◦ Enabled if the service is configured to run on boot. ◦ Disabled if the service is not configured to run on boot • Running Status: Displays ◦ Running if the service is running ◦ Stopped if the service is not running
Domain Status	Winbind Domain: Displays ◦ Not Joined if FortiNAC is not joined to any Active Directory through winbind ◦ Joined if FortiNAC is joined to the domain Domain Information: Displays the detailed information of the joined status of FortiNAC. ◦ This information may still show the previous join information if FortiNAC is no longer joined to the domain. In this case, the Winbind Domain will display “Not Joined” and the “Last Machine account password changed” date will show 1969 or 1970.
Details & Logs	• Service Status: Displays full details of the service status. ◦ Warnings such as ‘Unknown value ‘xxxxxx’ in section ‘yyyyyy’ can be ignored. • Service Log: Winbind log output • Systemd Log: Systemd journal output. Useful if winbind will not start for some reason.

Winbind Domain Configuration Details

Field	Description
Name	Unique name used to identify the configuration. Only alphanumeric characters and underscore are allowed.
Local NetBIOS Name	NetBIOS name by which the FortiNAC Samba server is known. For High Availability configurations, this is the primary FortiNAC Samba server. Example: FortiNAC FQDN = hostname.corp.example.com, Local NetBIOS Name = "HOSTNAME" Note: the maximum length for a NetBIOS name is 15 characters.
Secondary (HA) NetBIOS Name	NetBIOS name by which the FNAC Samba server is known. Note that the maximum length for a NetBIOS name is 15 characters. For high availability configurations, this is the primary FNAC Samba server.
Domain NetBIOS Name	NetBIOS name of your domain. This is the subdomain of the DNS domain name. Examples: Domain Controller Hostname = dc01.example.com, Domain NetBIOS Name = "EXAMPLE" Domain Controller Hostname = dc01.corp.example.com, Domain NetBIOS Name = "CORP"
Kerberos Realm Name	The DNS-style domain name. Example: "example.com"
Domain Controller Hostname	Name of the domain controller(s) Samba uses to do all its username/password validation. Important: Must always use Fully Qualified Domain Name (FQDN). See example below. Multiple servers may be specified, as well as * which will dynamically determine the best DC to contact. Examples: "dc01.example.com,dc02.example.com" "*" Requirements for additional Winbind instances for different domains • The DNS server that is used by FortiNAC and configured under the 'Config-Wizard' settings, must be configured with the DNS records for the additional Winbind instance of any additional domain added. • Ensure that DNS A record for the domain controller and DNS SRV records for LDAP and Kerberos are added to the DNS server configured in the FortiNAC Config-Wizard. For additional Winbind configuration information, see article " Create an additional Winbind instance for a second domain "
Log Level	The log level for the Winbind service. Recommended value is "none".
Join Domain	In order for Winbind authentication to work, FortiNAC must be joined to the domain. Configure the credentials for the account FortiNAC will use to join. • Username: User name FortiNAC uses to join the domain. Examples:

Field	Description
	trusted_user or trusted_user@example.com • Password: Password FortiNAC uses to join the domain • Keytab file: Select and upload a keytab file. This allows AD joins without needing to type in the admin account password for use by both RADIUS MSCHAPv2 authentication and Portal authentication using Kerberos.

Activity



Must be enabled in **RADIUS > Configuration > Activity Monitoring**.

The Network RADIUS Activity view (available when enabled in the Local Service view) displays RADIUS authentication activity on the network. This activity is tracked by periodically taking a snapshot that counts the recent access accept and reject responses and occurs in 5 minute intervals.

For rejected authentication requests, the failure counts are tracked by unique cause. This allows an administrator to see if there are any authentication problems on the network, especially if there are thousands of hosts logging in every day. A RADIUS dashboard widget also is available that provides a visual presentation of this activity in multiple, customizable formats.

Show Rejected Hosts

This opens a secondary view showing individual Access-Reject responses and shows for a given host MAC, and username the NAS IP address they attempted to authenticate on and the reason the request was rejected.

Service Connectors

This view acts as the main panel for creating and modifying connections and authentication between FortiNAC and different services.

Service	Description
MDM Servers	MDM Services allows configuring the connection or integration between FortiNAC and a Mobile Device Management (MDM) system. FortiNAC and the MDM system work together sharing data via an API to secure the network. FortiNAC leverages the data in the MDM database and registers hosts using that data as they connect to the network. For more information see MDM Servers on page 413. List of MDM servers supported by FortiNAC CA: - Air Watch - Fortinet EMS - Google GSuite

Service	Description
	JAMF MaaS360 MicrosoftIntune Mobile Iron Nozomi Citrix Endpoint Management
Emails/SMS	
Email Server	This allows FortiNAC to send emails to Administrators and network users. See Email settings on page 937 .
Authentication Sources	Service Connectors used to configure the connection between FortiNAC and the desired authentication server. The authentication source is used in the following use cases: • User registration • Captive Portal and Dissolvable Agent (see Global properties and Configure Authentication credentials) • Persistent Agent (see Credential configuration) • Import (see Import hosts users or devices) • Administration UI Login • Add Administrators (see Administrators) • Import Administrators (see Import an administrator)
Google Auth	See Google auth on page 407 .
Radius	See RADIUS on page 375
Syslog/Messaging	
Security Fabric Connection	See Security Fabric Connection on page 420

Authentication sources

There are two authentication sources in FortiNAC:

1. [Google auth on page 407](#).
2. [RADIUS on page 409](#)

Google auth

Google authentication allows users to authenticate using a Google account. When the settings are configured, the user logs into the network using their Google account instead of a username and password. When the user is authenticated, the user's email address (username and domain) is passed to FortiNAC to authenticate the user with the information.

Google Cloud Messaging for Android allows users to configure push notifications for the Mobile Agent.

You must first configure Google authentication through the Google Developer's Console. See [Google Developer's Console on page 407](#). Use the settings obtained during this process to configure Google authentication.



Important: The Captive Network Assistant feature (CNA) should not be configured in FortiNAC when using Google Authentication. Otherwise, HTTP errors may display on some devices when trying to authenticate. For details, see <https://support.google.com/accounts/answer/12917337?hl=en#zippy=%2Cdisallowed-useragent>

To disable CNA, see [Disabling Captive Network Assistant](#)

Settings

Field	Definition
Google account authentication	
Client ID	The value provided by Google that allows FortiNAC to perform Google authentication. The Client ID is generated during Google authentication configuration using the Google Developers Console.
Allowed domains	The domains that have access to the network through Google authentication.
Google Cloud Messaging for Android™	
Project number	The project number is generated during Google authentication configuration. When the device registers with FortiNAC, the Project number is sent to the agent on the device, which is then used to identify FortiNAC when the agent registers with Google to receive messages.
API key	The API key is a unique code that identifies FortiNAC to Google.

Google Developer's Console



These instructions are current as of 4/22/2026. See <https://developers.google.com/console/help/new/> for more information.

1. Log into <https://console.developers.google.com> using the Google account that you wish to use for FortiNAC integration.
2. Create a project (project number): https://support.google.com/cloud/answer/6251787?hl=en&ref_topic=6158848
3. Assign the project name.

4. Enter a unique project ID (e.g., FortiNAC<organization name>).
Note the project number, which is required during FortiNAC configuration.
5. Enable APIs: https://support.google.com/cloud/answer/6158841?hl=en&ref_topic=6262490
 - Enable Google + API.
 - Enable Google Cloud Messaging for Android API.
 - Enable Google People API
6. Configure Auth Client ID: https://support.google.com/cloud/answer/6158849?hl=en&ref_topic=6262490
 - Application Type, selection will be Web Application.
 - Authorized Javascript Origins: enter the URL for your FortiNAC Portal (https://<fortiNAC_FQDN>). This will be the origin of all Google authentication attempts.
Example: <https://myNAC.mycompany.org>
 - Authorized Redirect URIs: enter the URL for your FortiNAC Portal (should match Javascript Origin URL) URL's
Standard User Login: https://<fortiNAC_FQDN>/registration/ValidUserLogin.jsp
Custom Login: https://<fortiNAC_FQDN>/registration/CustomLogin.jsp
Game Console Registration Login: https://<fortiNAC_FQDN>/registration/GameRegister.jsp
Example for Standard user login authenticating with Google:
<https://myNAC.mycompany.org/registration/ValidUserLogin.jsp>
7. Configure the Server API Keys: https://support.google.com/cloud/answer/6158862?hl=en&ref_topic=6262490
 - Enter the effective external IP address of FortiNAC, and then click **Create**.
Note the API Key, which is required during FortiNAC configuration.

Add or modify account settings

1. Click **Network > Service Connectors**.
2. Click **Create New**.
3. Under **Authentication Sources**, select **Google Auth**.
4. Enter the Client ID obtained during Google authentication configuration. See [Google Developer's Console on page 407](#).
5. Click **+ next** to Allowed Domains to enter each domain that will have access to the network.
Note: It is not recommended that you use a common domain name, such as "google.com", because this will allow anyone with a generic Google account to have access to your network.
6. Click **OK**.
7. Click **System > Settings > Control > Allowed Domains**.
8. Add the following domains to the Allowed Domains list. These domains will allow access in isolation in order to authenticate through Google:
 - mail.google.com
 - apis.google.com
 - googleapis.com
 - schemas.google.com
 - accounts.google.com
 - ssl.gstatic.com

- `oauth.googleusercontent.com`
- `googlehosted.googleusercontent.com`

For each domain:

- Click **Add Domain**.
 - Enter the domain.
 - Click **Ok**.
- Once all domains have been added, click **Save Settings**.
 - Click **Portal > Portal Configuration > Global > Settings**.
 - Select **Social** from the appropriate Login Type drop-down menu to enable Google to be the default authentication method for that page. Available login types are:
 - Standard User Login
 - Custom Login
 - Game Console Registration Login
 - Click **Enable Google Auth**.
 - Click **Apply**. Google Sign In appears on the portal when the user accesses the network.

Enable push notifications

- Click **Network > Service Connectors**.
- Double click or Edit **Google Auth Service Connector**.
- Under **Google Cloud Messaging for Android**, enter the **Project Number** and **API Key** obtained during Google authentication configuration.
- Click **OK**.

RADIUS

The RADIUS Service Connector allows FortiNAC to authenticate users with a RADIUS account for user registrations and Administration UI access.

Field	Definition
Profile Name	Name displayed in the RADIUS server list. Name of the connection configuration for the connection between an MDM system and FortiNAC.
Host Name/IP Address	Host name or IP address of the RADIUS server.
RADIUS Secret	Encryption key used by the RADIUS server to send authentication information.
Authentication Port	Port number through which the RADIUS server communicates.
Accounting Port	Port number that the RADIUS server uses for the accounting features, if they are used. If your RADIUS server does not use accounting features, disable the field.
Validation Account	

Field	Definition
User Name	User name for verifying access to the RADIUS Server. This field is required, but only used when there are multiple RADIUS Servers configured. You must create an account on the RADIUS Server that is used by FortiNAC to communicate with that Server. The encryption method must be set to PAP.
Password	Password for verifying access to the RADIUS server. This field is required.

Email/SMS

This section covers the following:

- Email Server
- SMTP SMS Gateway
- REST SMS Gateway

Email server

This feature is available under Network > Connectors > Create New > Email/SMS > SMTP SMS Gateway.

For information on Email Server, see [Email Settings](#).

SMTP SMS Gateway

Adding SMTP SMS gateway

This feature is available under Network > Connectors > Create New > Email/SMS > SMTP SMS Gateway.

Feature	Description
Name	Name of the Messaging Gateway
Gateway Address (Email domain)	The provider's email domain, such as nextel.messaging.com
Country	Country to which this SMS Address corresponds. You may have providers that have a different SMS Address for each country in which they operate. You need a separate record for each one.
Prefix	Any numbers that are required before the user's mobile number. For example, you may have users that are in an adjacent country, therefore you may need to enter a number, such as 1, ahead of the mobile number.
Suffix	Any numbers required after the user's mobile number.
Max Message Length	Maximum allowed message length for each provider.
Enabled	Enables the Messaging Gateway.

Modifying SMTP SMS gateway

Once you add an SMTP SMS gateway, all SMTP SMS gateways are put under one card in Network > Service Connectors view under the name SMTP SMS gateway. To modify the gateway configuration that's been added, right click the Network > Service Connectors > SMTP SMS gateway card and search for the name of your gateway. Go to the configuration by clicking the pencil icon.

Deleting SMTP SMS gateway

To delete SMTP SMS gateway, right click the Network > Service Connectors > SMTP SMS gateway card and search for the name of your gateway. Go to the configuration by clicking the pencil icon. Delete the config by clicking delete button.

Configuring Global Max Message Length for SMTP SMS gateway

Right click the Network > Service Connectors > SMTP SMS gateway card and select Set Global Max Message Length.

REST SMS Gateway

Adding REST SMS gateway

This feature is available under Network > Connectors > Create New > Email/SMS > SMTP SMS Gateway.

Feature	Description
Name	Unique name of the SMS Gateway. A name may only be used once across all types of SMS Gateways.
API URL	API URL that is used to send SMS (Example: gateway.provider.com/sms/send).
HTTPS	Is the connection to the service HTTPS? If the Scheme is not included in the Gateway Address, the user has to specify it via the Toggle. Default is HTTP
HTTP Method	HTTP Method used to send SMS.
User Name	The User name that is used for HTTP basic Authentication to the gateway.
Password	The password that is used for HTTP basic Authentication to the gateway.
Content Type	Content Type used to contact the API URL.
Enabled	If Enabled, this SMS Gateway will appear in the list of Mobile Providers available to a user in both the Admin GUI and Portal. This is only a visual toggle, and the Gateway will still be used if a User has it selected as their Mobile Provider.
Form Parameters	These are various headers that are used to contact the API URL.



To make setting up a new gateway easier, FortiNAC ships with Twilio and Vonage based configuration settings under the names Twilio-example-config and Vonage-example-config. These configurations use placeholders which should be filled with details that are specific to the account.

Modifying REST SMS gateway

Once you add a REST SMS gateway, all REST SMS gateways are put under their own card in Network > Service Connectors view under the name you used while creating. To modify the gateway configuration that's been added, right click the Network > Service Connectors > "Name" card and go to the configuration by clicking **Edit**.

Deleting REST SMS gateway

To delete REST SMS gateway, right click the Network > Service Connectors > Name of the Gateway, and click **Delete**.

Testing REST SMS gateway connection

To test the REST SMS gateway connection, you can right click the Network > Service Connectors > Name of the Gateway, and test the config by clicking **Test Connection**.

You can also **edit** the configuration and test the connection once you are in the configuration window.

Once the test connection overlay is opened, select the user with which you wish to test the connection.

The user has to be configured with the phone number and the messaging gateway that you wish to test the connection with. Remember to include the country code for the phone number.

Note: Remember to save the configuration before actually trying to test the connection.

REST SMS gateway can be used at all places where SMTP SMS gateways are used to send the SMS.

Setting Default REST SMS gateway

To set a REST SMS gateway as Default, right click the Network > Service Connectors > Name of the Gateway, and set the configuration as default by clicking **Set as Default**.

Debug options

To debug, enable debugging in the CLI and the user should be able to see what the Request was and its corresponding response from output.master.

```
FortiNAC FNMCA
root@samnac:/bsc
> nacdebug -name MessagingGatewayPlugin true

Setting MessagingGatewayPlugin debug to true

Select sam@e4b97a542cc4:/mnt/c/Users/student

yams.MessagingGatewayPlugin FINER :: 2022-02-28 15:20:29:970 :: #758 :: REST request = POST https://api.twilio.com/2010-04-01/Accounts/AC8a1224bac2c71439091af40e7a092aef/Messaging.json HTTP/1.1
yams.MessagingGatewayPlugin FINER :: 2022-02-28 15:20:30:303 :: #758 :: REST response = HttpResponseProxy{HTTP/1.1 201 Created [Date: Mon, 28 Feb 2022 20:29:48 GMT, Content-Type: application/json, Content-Length: 820, Connection: keep-alive, Twilio-Concurrent-Requests: 1, Twilio-Request-Id: RQ2979db051ef499d8a73df9e5eb2a5fb6, Twilio-Request-Duration: 0.129, Access-Control-Allow-Origin: *, Access-Control-Allow-Headers: Accept, Authorization, Content-Type, If-Match, If-Modified-Since, If-None-Match, If-Unmodified-Since, Access-Control-Allow-Methods: GET, POST, DELETE, OPTIONS, Access-Control-Expose-Headers: ETag, Access-Control-Allow-Credentials: true, X-Powered-By: AT-5000, X-Shenanigans: none, X-Home-Region: us1, X-API-Domain: api.twilio.com, Strict-Transport-Security: max-age=31536000] ResponseEntityProxy{[Content-Type: application/json, Content-Length: 820, Chunked: false]}}
```

MDM Servers

MDM Services allows you to configure the connection or integration between FortiNAC and a Mobile Device Management (MDM) system. FortiNAC and the MDM system work together sharing data via an API to secure the network. FortiNAC leverages the data in the MDM database and registers hosts using that data as they connect to the network. Any updates to the MDM service connector on Network Control Manager(NCM) will be synchronized to FortiNAC CA to ensure update to-date connector information with accurate management visibility.

The MDM Service Connector can be configured either on the FortiNAC Manager or the individual managed FortiNAC servers. Choose the appropriate option based upon which FortiNAC servers require the MDM host record information.

Option 1

Requirement: All servers managed by FortiNAC Manager require MDM host record information.

Configuration: Configure the MDM Service Connector on the FortiNAC Manager. No other configuration is required.

Behavior: The Manager copies all MDM host record information to the servers after each MDM poll.

Benefit: Provides a single point of contact for the MDM server. Reduces the overall number of queries the MDM server has to process.

Option 2

Requirement: Only certain FortiNAC servers require MDM host record information.

Configuration: Configure the MDM Service Connector on the FortiNAC servers requiring the data.

Behavior: The MDM server is polled by each FortiNAC server configured with the MDM Service Connector.



Proxy communication is not supported.

Supported vendors

- Air Watch
- Fortinet EMS
- Google GSuite
- JAMF
- MaaS360
- MicrosoftIntune
- Mobile Iron
- Citrix Endpoint Management

For more information about supported vendors, refer to the appropriate reference manual in the the Fortinet Documentation Library:

- Fortinet EMS: [FortiClient EMS Device Integration](#)
- All others: [Third Party MDM Device Integration](#)

Settings

Field	Definition
MDM Vendor	Name of the vendor of the MDM system.
Name	Name of the connection configuration for the connection between an MDM system and FortiNAC.
Request URL	The URL for the API to which FortiNAC must connect to request data. This will be a unique URL based on your MDM system.
Identifier	A type of key used to identify FortiNAC to the MDM server. This field is not required for all MDM products. In the case of AirWatch, this is the API Key generated during the AirWatch Configuration. An API key is a unique code that identifies the FortiNAC server to AirWatch and is part of the authentication process for AirWatch.
Application ID	Enter the application ID.
Platform ID	Enter the platform version number.
Application Version	Enter the application version number.
Access Key	Enter the application access key (API key).
Enable Delegated Permissions	If enabled, API permissions are delegated by a signed-in user. When disabled, API permissions are configured and granted in the MDM application registration portal (recommended configuration). Note: Existing MS Intune connectors created prior to versions 9.1.6/9.2.3/9.4.0 will have this setting enabled.
User ID	User name of the account used by FortiNAC to log into the MDM system when requesting data.
Password	Password for the account used by FortiNAC to log into the MDM system when requesting data. This field displays only when adding a new MDM connection configuration. It is not displayed in the table of MDM servers.
Poll Interval	Indicates how often FortiNAC should poll the MDM system for information.
Last Poll	Date and time of the last poll.
Last Successful Poll	Date and time of the last poll that successfully retrieved data.
Create Date	Date that this connection configuration was set up.
On Demand Registration	If enabled, when an unknown host reaches the captive portal, FortiNAC queries the MDM server for information about that host. If the host exists in the MDM server, it is registered in FortiNAC using the data from the MDM server.

Field	Definition
Revalidate Health Status On Connect	If enabled, when the host connects to the network FortiNAC queries the MDM server to determine if the host is compliant with MDM policies. This setting is disabled by default. When enabled, the MDM may not be able to manage the rate of queries from FortiNAC, causing performance issues. Instead of enabling Revalidate Health Status On Connect, you can enable automatic registration polling to occur once a day, which will also retrieve Health Status, but with less frequency.
Enable Automatic Registration Polling	If enabled, FortiNAC will automatically poll the MDM server for information. The server responds to the poll with all devices in its database. Devices returned from the poll are automatically registered and identified as being managed by the MDM server. Currently there is no way of filtering or controlling which devices are processed by FortiNAC.
Remove Hosts	If enabled, when FortiNAC polls the MDM server it deletes hosts from the FortiNAC database if they have been removed or disabled on the MDM server.
Update Applications	If enabled, when FortiNAC polls the MDM server it retrieves and stores the Application Inventory for hosts that are in the FortiNAC database. This setting is disabled by default. When enabled, the MDM may not be able to manage the rate of queries from FortiNAC, causing performance issues.
Last Modified By	User name of the last user to modify the connection configuration.
Last Modified Date	Date and time of the last modification to this connection configuration.
Credential JSON	GSuite: (Introduced in FortiNAC version 9.4) Imports the Service Account Key JSON file downloaded from the Google Developers Console. 1) Select the "Modify Credential JSON" button. 2) Populate the Credential JSON field with the Service Account Key file downloaded from the Google Developers Console. This can be done in two ways: Option 1 (Recommended): Click Browse and select the file. It's contents will appear in the Credential JSON window. Option 2: Copy and paste the file contents.
Update Hosts Role (Versions F 7.2.9 +, F 7.4.2 + and F 7.6.3 +)	Use the Ownership value from the MDM record to determine the FortiNAC Host Role. The Host Role is only overridden for hosts with NAC-Default role or no assigned role. Not available for all MDM service connectors. See Third Party MDM Device Integration.
Right click options	
Delete	Deletes the MDM Service.
Modify	Opens the Modify MDM Service dialog.
Poll Now	Polls the MDM server immediately.
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746 .

Field	Definition
	 You must have permission to view the admin auditing log. See Add an administrator profile on page 139.
Test Connection	Tests the connection between the selected MDM server and FortiNAC. Error messages indicate which fields are missing or incorrect.
Buttons	
Add	Opens the Add MDM Service dialog.
Modify	Opens the Modify MDM Service dialog.
Test Connection	Tests the connection between the selected MDM server and FortiNAC. Error messages indicate which fields are missing or incorrect.
Poll Now	Polls the MDM server immediately.

Add or modify MDM service

1. Go to **Network > Service Connectors**
2. Select **Create New** and select a vendor or **Edit** an existing MDM Server.
3. Use the settings for the MDM Services to enter the MDM Service information.
4. Click **OK** to save.



The Revalidate Health Status On Connect and Update Applications settings are disabled by default. When enabled, the MDM may not be able to manage the rate of queries from FortiNAC, causing performance issues.



Instead of enabling Revalidate Health Status On Connect, you can enable automatic registration polling to occur once a day, which will also retrieve Health Status, but with less frequency.

Delete MDM service

1. Go to **Network > Service Connectors**
2. Select an **MDM Service** record from the table.
3. Click **Delete** at the top of the view.
4. Click **Yes** on the confirmation message.

OT

OT Service Connector allows you to configure the connection or integration between FortiNAC and an Operational Technology (OT) security system. FortiNAC and the OT security system work together sharing data via an API to secure

the network. FortiNAC leverages the data in the OT security system’s database and registers hosts using that data as they connect to the network.

The OT Service Connector is configurable on the FortiNAC Manager or the individual managed FortiNAC servers. Choose the appropriate option based upon which FortiNAC servers require the OT host record information.

Option 1

Requirement: All servers managed by FortiNAC Manager require OT host record information.

Configuration: Configure the OT Service Connector on the FortiNAC Manager. No other configuration is required.

Behavior: The Manager copies all OT host record information to the servers after each OT poll.

Benefit: Provides a single point of contact for the OT security system. Reduces the overall number of queries the OT security system has to process.

Option 2

Requirement: Only certain FortiNAC servers require OT host record information.

Configuration: Configure the OT Service Connector on the FortiNAC servers requiring the data.

Behavior: The OT security server is polled by each FortiNAC server configured with the OT Service Connector.



Proxy communication is not supported.

Supported vendors

- [Nozomi](#)
- [Claroty](#)

For more information about supported vendors, refer to the [Third Party OT Security Device Integration](#) reference manual in the Fortinet Documentation Library

Settings

Field	Definition
Name	Name of the connection configuration for the connection between an OT security system and FortiNAC.
Request URL	The URL for the API to which FortiNAC must connect to request data. This will be a unique URL based on your OT security system.
User ID	User name of the account used by FortiNAC to log into the OT security system when requesting data.
Password	Password for the account used by FortiNAC to log into the OT security system when requesting data. This field displays only when adding a new service connection configuration. It is not displayed in the table of OT security systems.

Field	Definition
Enable Automatic Registration Polling	If enabled, FortiNAC will automatically poll the OT security system for information
Automatic Registration Polling Interval	Indicates how often FortiNAC should poll the system for information when Automatic Registration Polling is enabled. Interval can be set for Days, Hours or Minutes.
Remove Hosts Deleted	If enabled, when FortiNAC polls the OT security system, it deletes hosts from the FortiNAC database if they have been removed from the system.
Poll OT Assets Only	Only poll Claroty assets with class type of OT. FortiNAC host records for other class types like IT will not be created.
Poll Approved Assets Only	Only poll Claroty assets that have an approved value of "true." FortiNAC host records will not be created for Claroty assets with a "false" or non-existent approved value.
Enable On Demand Registration	If enabled, when an unknown host reaches the captive portal, FortiNAC queries the OT security system for information about that host. If the host exists in the OT security system, it is registered in FortiNAC using the data from the OT security system.
Revalidate Health Status On Connect	If enabled, when the host connects to the network FortiNAC queries the OT security system to determine if the host is compliant with OT security system policies. This setting is disabled by default. When enabled, the OT security system may not be able to manage the rate of queries from FortiNAC, causing performance issues. Instead of enabling Revalidate Health Status On Connect, you can enable automatic registration polling to occur once a day, which will also retrieve Health Status, but with less frequency.
Compliance Level	None: Claroty assets will not be evaluated for OT compliance in FortiNAC. Medium, High or Critical: Claroty assets with a Medium risk_level 1, High risk_level 1 or Critical risk_level 3 will be marked as not MDM compliant in FortiNAC. High or Critical: Claroty assets with a High risk_level 1 or Critical risk_level 3 will be marked as not MDM compliant in FortiNAC. Critical Only: Claroty assets with a Critical risk_level 3 will be marked as not MDM compliant in FortiNAC.
Disable Hostname Verification	If enabled, SSL Hostname Verification will be disabled.
Right click options	

Field	Definition
Delete	Deletes the OT Service.
Edit	Opens the Modify OT Service dialog.
Buttons	
Create New	Opens the Add OT Service dialog.
Edit	Opens the Modify OT Service dialog.
Delete	Deletes the OT Service.

Add or modify MDM service

1. Go to **Network > Service Connectors**.
2. Select **Create New** and select a vendor or **Edit** an existing OT security system.
3. Use the settings for the OT Services to enter the OT Service information.
4. Click **OK** to save.



The Revalidate Health Status On Connect and Update Applications settings are disabled by default. When enabled, the MDM may not be able to manage the rate of queries from FortiNAC, causing performance issues.



Instead of enabling Revalidate Health Status On Connect, you can enable automatic registration polling to occur once a day, which will also retrieve Health Status, but with less frequency.

Delete MDM service

1. Go to **Network > Service Connectors**.
2. Select an **OT Service record** from the table.
3. Click **Delete** at the top of the view.
4. Click **Yes** on the confirmation message.

Nozomi

See the [Nozomi](#) section of the [Third Party OT Security Device Integration](#) reference manual.

Claroty

See the [Claroty](#) section of the [Third Party OT Security Device Integration](#) reference manual.

Security Fabric Connection

The Fortinet Security Fabric provides an intelligent architecture that interconnects discrete security solutions into an integrated whole to detect, monitor, block, and remediate attacks across the entire attack surface. It delivers broad protection and visibility into every network segment and device, be they hardware, virtual, or cloud based.

- The physical topology view shows all connected devices, including access layer devices. The logical topology view shows information about the interfaces that each device is connected to.
- Security rating checks analyze the Security Fabric deployment to identify potential vulnerabilities and highlight best practices to improve the network configuration, deploy new hardware and software, and increase visibility and control of the network.
- Fabric connectors provide integration with multiple SDN, cloud, and partner technology platforms to automate the process of managing dynamic security updates without manual intervention.
- Automation pairs an event trigger with one or more actions to monitor the network and take the designated actions automatically when the Security Fabric detects a threat.

Currently supported features:

- Physical Topology view
- Quarantine via FortiNAC action: Users can configure an automation stitch with the "Quarantine via FortiNAC" action with a Compromised Host or Incoming Webhook trigger. When the automation is triggered, the client PC will be quarantined and its MAC address is disabled in the configured FortiNAC. For instructions on configuring this feature in the FortiGate, see section [Quarantine via FortiNAC action](#) of the 6.4.2 Administration Guide.

Add FortiNAC to the Security Fabric:

1. In the FortiNAC Administration UI, navigate to **Network > Service Connectors**.
2. Click **Create New**.
3. Click **Security Fabric Connection**.
4. Enter the following values and save: IP: Root FortiGate IP address Port: 8013
Refer to the FortiNAC Security Fabric / SSO integration guide for complete details and configuration.
<https://docs.fortinet.com/document/fortinac-f/7.6.0/security-fabric-ss0/404237/overview>

ServiceNow ITSM Integration

FortiNAC integrates with ServiceNow IT Service Management (ITSM) to automatically create ServiceNow incidents from FortiNAC alarms generated by Event > Alarm mappings. The integration is delivered as a Log Receiver/Messaging connector so that alarm notifications can be routed to ServiceNow alongside other targets (e.g., FortiAnalyzer, SNMP Trap, Syslog CEF/CSV). The connector supports OAuth 2.0 and API Key authentication and follows existing FortiNAC HA and Manager design patterns (1+1, N+1, CA cluster, and NCM clustering).

Workflow

1. An Event occurs in FortiNAC and is evaluated by **Event > Alarm** mappings.
2. If matched, FortiNAC raises an **Alarm** with severity/metadata.
3. The **Alarm** is sent to the selected Log Receiver(s) under the Log Receivers / Messaging category.
4. For the ServiceNow ITSM receiver, FortiNAC formats an incident payload (e.g., Short Description, Impact/Severity mapping, timestamp) and sends it to ServiceNow via REST (Table API).
5. ServiceNow creates an Incident; operators triage and resolve within ITSM while FortiNAC remains the authoritative event source.

Authentication & security

The connector supports two auth modes:

- **OAuth 2.0:** Use a REST API Auth Scope (Table API v1, resource `/now/v1/table/{tableName}`) and an OAuth Application Registry. Acquire tokens via the instance token endpoint (`oauth_token.do`) using password or refresh_token grants.
- **API Key:** Use an access key associated with your ServiceNow instance.

Note: Choose OAuth 2.0 where possible for better lifecycle and rotation controls.

Pre-Configuration: Setting up OAuth in ServiceNow

Create the REST API Auth Scope

1. Go to **System Web Services > API Auth Scopes > REST API Auth Scope**.
2. Click **New** to create a new **Auth Scope**.
3. Give a **name** to the Auth Scope.
4. Set the value of REST API to **"Table API"**.
5. **Unselect** both **"Apply auth scope to all versions in this API"** as well as **"Apply auth scope to all resources in this API."**
6. Ensure that the REST API Version field is set to **"v1"**.
7. Ensure that the Resource field is set to **"/now/v1/table/{tableName}"**.
8. **Click** on the **Search icon** next to Auth Scope.
9. **Create** a new **Auth Scope** or use an existing one if needed.
10. **Click** on the green check mark to **save** the Auth Scope.
11. Submit the **REST API Auth Scope**.

Create an Application Registry

1. Go to **System OAuth > Application Registry**.
2. **Click New** and select **"Create an OAuth API endpoint for external clients"**.
3. Give a **name** to the Application Registry.
4. Optionally fill in the Client Secret field.
5. **Click** on the Search icon next to Auth Scope and **select** the **Auth Scope** created in the previous step.
6. **Submit** the **Application Registry**.
7. **Re-open** the **Application Registry** and **copy** the **Client ID** and **Client Secret**.

Use these values in FortiNAC when setting up the ServiceNow ITSM service connector.

Create an Oauth Application Registry in ServiceNow

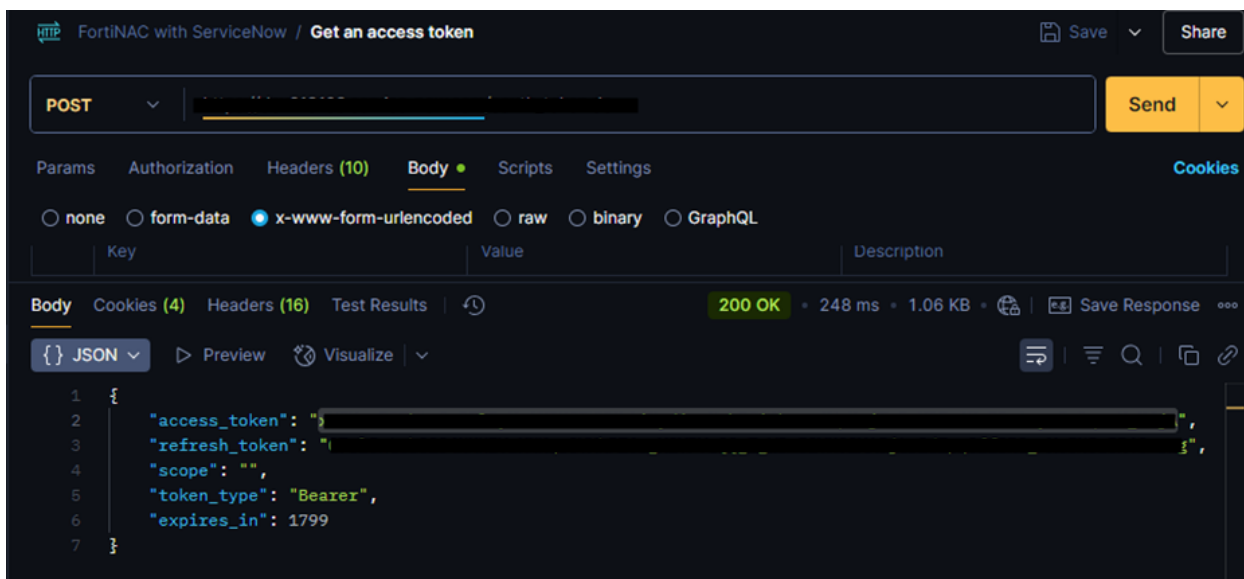
1. **Open** your web browser and **navigate** to your ServiceNow instance URL.
2. Navigate to **Application Registry**
3. Create a **New OAuth Application** and fill in the **Application** details.

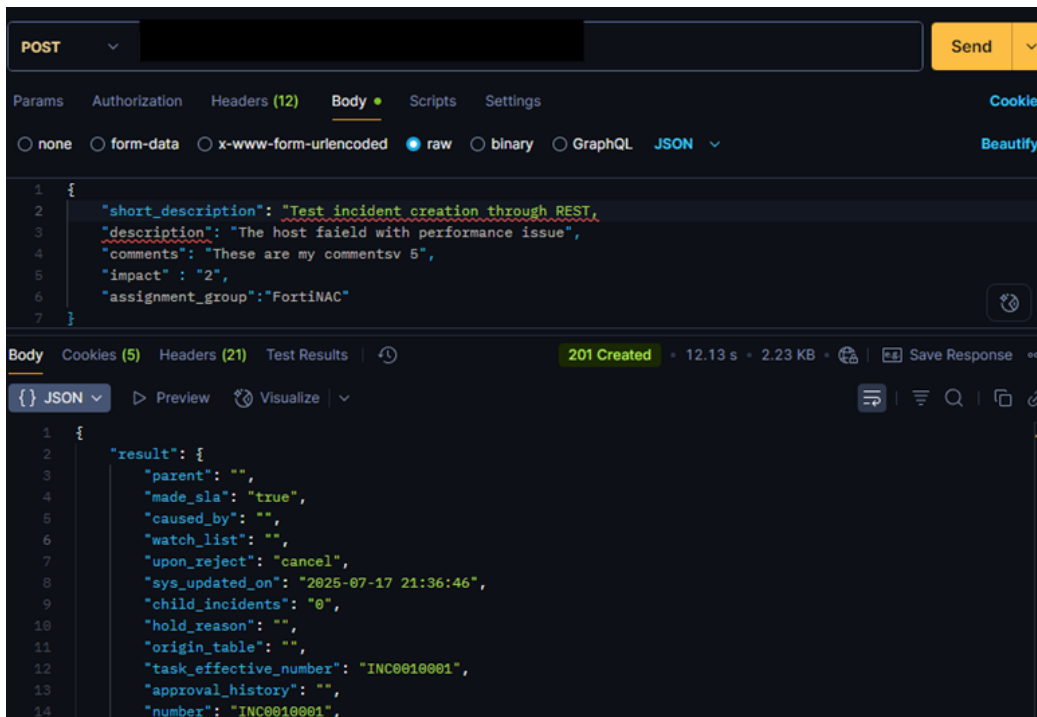
Get the Access Token

Use the information below in your OAuth authentication process to get an access token for accessing the ServiceNow API.

- **Endpoint URL:** <instance -name>.service-now.com/oauth_token.do
- **Grant_type:** required, the type of credentials authorizing the request for an access token, this parameter must have a value of either password or refresh_token.
Password:
Refresh_token:
- **Client_id:** required
- **Client_secret:** required
- **Username:** the user account name authorizing the access token request.
- **Password:** the password for the user account authorizing the access token request. This parameter is required for access token requests with a grant_type of password.
- **refresh_token:** the existing refresh token authorizing the access token request.

Example





The pre-configuration is now complete.

Configuration

1. Go to **Network > Service Connectors**.
2. Click **Create New**.
3. Click **ServiceNow Incidence**.
4. Add the **Authentication type**. Use the information created in the pre-configuration.
5. Added "ServiceNow ITSM" should show on the Service Connector Page.

The "ServiceNow ITSM" record will automatically display in the Log receiver when a "ServiceNow ITSM" is added on the Service Connector Page.

FortiEdge Cloud

This feature can be found in **Network > Service Connectors > FortiEdge Cloud**.

FortiAP has three wireless management topologies (integrated via FortiGate, FortiEdge Cloud, or dedicated controller), currently FortiNAC is supporting the first two topologies: Integrated via Fortigate and FortiEdge Cloud.

FortiEdge Cloud is a unified management platform for standalone FortiAP and FortiSwitch deployments. When FortiAPs are registered with FortiEdge Cloud, wireless configurations and endpoint discovery are managed by the FortiEdge Cloud. This allows users to manage FortiAP's without requiring a FortiGate

Configure FortiEdge Cloud integration on FortiNAC

To build a connection between FortiNAC and FortiEdge Cloud, a FortiEdge Cloud service connector will be required.

After the FortiEdge Cloud account has been added to FortiNAC service connector, FortiNAC will be able to support endpoint visibility and access control.

Steps

1. Go to **Network > Service Connectors**. Click **Create New** and add **FortiEdge Cloud** as a service connector.
2. Configure the following:

Field	Description
Connector settings	
Name	You can specify this service connector name here.
API URL	The URL for the FortiEdge Cloud service, the default is used for local/US-based customers.
User Type	Choose user type on FortiEdge Cloud. (Email, IAM, API)
Account ID	FortiEdge Cloud account ID. Note: Account ID can be found on the right side of the dashboard. The screenshot shows the FortiEdge Cloud dashboard. In the top right corner, there is a user profile dropdown menu. A red rectangular box highlights the 'Account ID' field within this menu, which contains the text 'Account ID: account_1234567890'. The dashboard also displays various metrics like 'Managed network elements', 'Client devices connected to', 'High CPU Utilization', 'High Memory', 'Access Points', 'SSIDs', 'Clients', and 'Data Usage'.
User ID	FortiEdge Cloud user account
Password	FortiEdge Cloud user password
Connect	Click to check connection status.
Discovery settings	
Container	Click the dropdown list to choose an existing container or leave it empty. If it is left empty, a container called "FortiEdge Cloud" will be generated automatically.
Managed Networks	Type the network in FortiEdge Cloud that needs to be managed.
Enable Automatic polling	Automatic poll service connector to update network, AP, SSID info. The default automatic polling interval is 1 hour.
Advanced settings	
Connect Timeout:	Total time to wait to connect to FortiEdge Cloud (defaults is 10 secs).
Read Timeout	Total time to wait for FortiEdge Cloud to respond (defaults is 10 secs).
Debug	Enables debug for this service connector.

Your FortiEdge Cloud Service Connector should be created.

Inventory

Once the service connector has been successfully created and polled, the container with managed FortiEdge Cloud network and AP as well as SSIDs will be discovered and shown in **Network > Inventory**.

SSID can be configured by double clicking on the SSID.

VLAN's can be created on FortiNAC. After polling, it will automatically be added to the FortiEdge Cloud network model as virtual ports.

To create and assign a VLAN on FortiNAC

1. To create VLAN on FortiNAC, navigate to Network **>Inventory**, right click the FortiEdge Cloud network, choose **Model Configuration**.
(optional) Model configuration can also be entered here in SSID configuration.
2. In Model configuration, click **Add** under Access Enforcement Descriptions and enter the VLAN ID to add additional access values.
3. Navigate to FortiEdge Cloud network, choose the SSID and double click it; after polling, access values can be chosen for different host state.

Additional features

Test connector status and Poll FortiEdge Cloud

Once the service connector has been created successfully, the user can right click to edit the current configurations, delete the service connector, or poll and test connection.

Steps

1. Go to **Network > Service Connectors**, where the FortiEdge Cloud should be visible.
2. **Right click** Test Connection to test if the FortiEdge Cloud account has been added successfully.
3. Click **Poll** for FortiEdge Cloud network, AP and SSID changes.



See the [FortiEdge Cloud Integration Guide](#).

Arista Cloud

FortiNAC provides network visibility (where endpoints connect) and manages network access for wireless endpoints connecting to Access Points managed by the Arista Cloud Wireless Controller. FortiNAC supports individual SSID configuration and management for this device.

For more information, see the [Arista Wireless Integration manual](#).

Check Point Cloud

FortiNAC controls access to the remote user's device connecting over the VPN. In order for the device to be able to gain access the network, FortiNAC must know about the connecting device and verify the device is in good standing.

1. When a device initially connects over a VPN tunnel, the device is restricted.
2. FortiNAC identifies the device as known and trusted.
3. The device is unrestricted.
4. If configured for endpoint compliance, the device's security posture is evaluated. Network access is restricted upon failure.

Relevant Documentation

[Check Point VPN Integration \(Central Mode\)](#)

[Check Point VPN Integration \(Local Mode\)](#)

Meraki Cloud

FortiNAC provides network visibility (where endpoints connect) and manages network access for wireless endpoints connecting to Access Points managed by the Meraki Cloud Wireless Controller. FortiNAC supports individual SSID configuration and management for this device.

For more information, see the [Meraki Service Connector Guide](#).

Mist Cloud

FortiNAC provides network visibility (where endpoints connect) and manages network access for wireless endpoints connecting to Access Points managed by the Mist Cloud Wireless Controller. FortiNAC supports individual SSID configuration and management for this device.

For more information, see the [Mist Wireless Integration](#).

Admin SAML SSO

Available in FortiNAC vF 7.6.3 +

Enables administrators to log in to the FortiNAC administrative UI using IdP credentials.

For more information, see the [SAML SSO integration](#).

User SAML SSO

Available in FortiNAC vF 7.6.3 +

Enables end users to authenticate through the Captive Portal using IdP credentials.

For more information, see the [SAML SSO integration](#).

Vulnerability Scanners

Overview

What It Does

FortiNAC integrates with third-party vulnerability scanners to retrieve the scan results as well as device details for targeted hosts. Scans can be created either from FortiNAC or the vulnerability scanner.

How It Works

FortiNAC supports integration with vulnerability scanners via service connector. Once configured, FortiNAC can retrieve scan results from supported vulnerability scanners. Currently, two vulnerability scanners are supported: **Tenable** and **Qualys**.

Through the integration, FortiNAC can retrieve detailed vulnerability scan results for target hosts. In addition, FortiNAC collects device information such as device ID, device location, and firmware versions of scanned devices.

Requirements

- A valid vulnerability scanner account with active license (Tenable or Qualys)
- A properly configured service connector in FortiNAC with correct account settings.

For configuration details, please refer to [Vulnerability Scanner Guide](#).

Processing scan results

At each Vulnerability Scanner poll, FortiNAC retrieves and processes the results for each configured scan that has completed since the previous poll of the scanner. Multiple scans can target a host. If any host's scan result exceeds the scan's failure threshold configured in FortiNAC, the host will be identified as failing scan.

Host View Columns

Host View Column	Description
Vulnerability Scan Status	Indicates the host's current health status
Last Vulnerability Scan	Displays the most recent time/date when scan results were processed for the host.
Vulnerability Details	Displays the detail vulnerability level and score.
Vulnerability Scan Status	Showing if the host pass or fail the scan.
Vulnerability Source	Indicates the name of the scan.

Also, Device ID, Device Location and Firmware Version can be retrieved from the vulnerability scan.

The vulnerability scan filters in the custom filters of the Host/Adapter Users views allow you to display hosts by Failed Scan, Passed Scan, or Not Scanned status. You can also display hosts that were scanned before, during, or after a specified time period. To configure the vulnerability scan filters for a host, see [Settings](#).

The Show Events option of a host filters events from the Events Log for the selected host. When results exceed the failure threshold, a Vulnerability Scan Failed event is generated. When the host's scan results do not exceed the failure threshold, a Vulnerability Scan Passed event is generated. The date and time displayed in the message for a Vulnerability Scan Failed or Vulnerability Scan Passed event indicates when the vulnerability scanner scanned the host. See [Events](#).

The following table lists the events that may be generated when the scan results are processed.

Events generated when FortiNAC processes scan results for hosts.	
Vulnerability Scan Failed	The host failed the vulnerability scan.
Vulnerability Scan Passed	The host passed the vulnerability scan.
Vulnerability Scan Started	The vulnerability rescan has started.
Vulnerability Scan Finished	The vulnerability rescan has finished.

Events generated when FortiNAC processes scan results for hosts.

Events generated for interaction between FortiNAC and the vulnerability scanner.

Vulnerability Scan Ignored	Scan results from the vendor include hosts that were added to the Vulnerability Exceptions Group, indicating which hosts were ignored. Hosts in this group are allowed onto the network, regardless of scan results.
Vulnerability Scan Incomplete	FortiNAC polls the vendor for scan results for a configured scan, but scan results are unavailable because the scan was not run by the vendor.
Vulnerability Scan Request Refused (Qualys Integration only)	The IP address targeted by a rescan is not included in the list of Qualysasset IPs.
Vulnerability Scan Removed	A Vulnerability scan that was added to FortiNAC was removed from the vulnerability scanner.
Vulnerability Scan Skipped	The Vulnerability scanner has not run the scan since FortiNAC previously polled it, so FortiNAC skipped the scan during processing.
Vulnerability Scanner Concurrent API Limit Exceeded (Qualys Integration only)	Exceeded the limit that is set for the number of requests that can be processed concurrently.
Vulnerability Scanner Connection Failure	The connection to the vulnerability scanner has failed.
Vulnerability Scanner Deleted	A vulnerability scanner was deleted from FortiNAC.
Vulnerability Scanner Periodic API Limit Exceeded (Qualys Integration only)	Qualys rejected an API request because the periodic API limit has been exceeded. The event message includes the number of seconds until the scanner will accept an API request.

These events can be enabled or disabled. For more information, see [Enable and disable events on page 773](#).

Vulnerability scan results enforcement

In order to force hosts which have failed Vulnerability scans to remediate, use an administrative scan mapped to the **Vulnerability Scan Failed** and the **Vulnerability Scan Passed** events, with **Host Security** actions of **At Risk** and **Safe**, respectively. See [Add a scan on page 616](#).

When the host fails the scan

In order to isolate hosts that have failed the vulnerability scan, configure an event to alarm mapping for the **the Vulnerability Scan Failed** event.

1. Create a host security action and add the **Mark Host At Risk** activity for the **Admin Scan**.
2. Map the **Vulnerability Scan Failed** event to the **Security Action**. Select **Host Security Action**, choose **At Risk**, and then select the **Admin Scan**. See [Add or modify alarm mapping on page 787](#).
3. To customize the vulnerability scan information displayed on the Remediation Portal page, edit the content in the **Global > Failure Information** page in the portal content editor.

When the host passes the scan

To move the host to production when the host passes the vulnerability scan, configure an event to alarm mapping for the **Vulnerability Scan Passed** event, with a **Host Security Action** of **Safe** for the administrative scan.

1. Create a host security action and add the **Mark Host Safe** activity for the **Admin Scan**.
2. Map the **Vulnerability Scan Passed** event to the **Security Action**. Select **Host Security Action**, choose **Safe**, and then select the **Admin Scan**. See [Add or modify alarm mapping on page 787](#).

Exceptions

Hosts that are added to the vulnerability scanner Exceptions Group are allowed onto the network even if the vulnerability scan fails. Failed vulnerability scans for hosts in this group will not be listed in the Remediation Portal page, and this page will not appear if a host in this group fails a vulnerability scan, but passes all other scans. For hosts in the vulnerability scanner exceptions group, the **Vulnerability Scan Status** column will always display **Passed** in the Host View.

Remediation

If the host fails a vulnerability scan, the Remediation Portal page will show details for the vulnerability scan that failed. Users can click the scan to see details of the failed scan provided by the vulnerability scanner, and solutions to fix the vulnerability. After remediation, users click **Rescan** to rescan the host. If a host fails for multiple vulnerability scans when FortiNAC performs a "Poll Now" of the vulnerability scanner, if you are enforcing access and using an Admin Scan with a Host Security Action to mark the host "at risk", each scan failure and rescan m be performed separately because each scan failure triggers an event/alarm that is unique to one scan.

Settings

Field	Definition
Name	The name of the scanner to be displayed in FortiNAC.
Request URL	The URL for retrieving scan results from the vulnerability scanner (typically in the format of https://<IP>:####).
User Name	The username for retrieving scan results from the vulnerability scanner.
Vendor	The vendor of the vulnerability scanner.
Poll Interval	The interval for how often FortiNAC retrieves scan results from the Vulnerability scanner.
Last Successful Poll	The last time FortiNAC successfully retrieved scan results from the Vulnerability scanner.
Last Modified By	The user who last modified the Occurs when a Vulnerability scanner was deleted from FortiNACVulnerability scanner configuration.
Last Modified Date	The date when the FortiNAC Vulnerability scanner configuration, as defined in FortiNAC, was last modified.
Right click options	
Modify	Modifies the selected vulnerability scanner configuration.

Field	Definition
Delete	Deletes the selected vulnerability scanner.
Test Connection	Tests the connection between FortiNAC and the vulnerability scanner.
Poll Now	Immediately polls selected vulnerability scanner for new scan results, instead of waiting for the poll interval.
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746 .
 You must have permission to view the admin auditing log. See Add an administrator profile on page 139.	

Add or modify a vulnerability scanner

When you add or modify a vulnerability scanner, you are configuring the connection to the FortiNAC Vulnerability scanner.

1. Select **System > Settings**.
2. Expand the **System Communication** folder.
3. Select **Vulnerability Scanners**.
4. Click **Add** or select an existing scanner from the list and click **Modify**.
5. Use the table below to enter the vulnerability scanner information in the **General** tab.

Field	Definition
Vendor	The vendor of the Vulnerability scanner.
Name	Enter a name for the scanner to be used in FortiNAC.
Request URL	The URL for retrieving scan results from the vulnerability scanner.
User Name	Enter the username for retrieving scan results.
Password	Enter the password for retrieving scan results.
Poll for Scan Results Every	Defines how often FortiNAC retrieves results from the vulnerability scanner.
Test Connection	Click to test the connection between FortiNAC and the vulnerability scanner.

6. Click the **Scans** tab.
7. Select the scan(s) in the Available Scans list and click the down arrow to add the scan(s) from the list of available scans on the vulnerability scanner to the selected scans list which FortiNAC will process. Click the double arrow to add all scans to the Selected Scans list. FortiNAC will only process results for scans in the Selected Scans list.
8. Select a scan in the Selected Scans list, and then click **Set Failure Thresholds**.
9. Select the check box next to each category where you wish to enter a threshold value.
10. Enter the minimum number of vulnerabilities for each category that may occur in the scan results before the host is identified as failing the scan. For example, entering "5" in the "Medium" category means that if five or more Medium vulnerabilities are detected when the host is polled, the host will be marked as Failed for that scan.



Categories are vendor-specific.

11. Click **OK**.
12. To remove a scan from the **Selected Scans** list, click the scan and then click **Delete**. The scan is returned to the **Available Scans** list.

Qualys Scanner Integration

Qualys requires an in-network scanner host for scans. When Qualys is selected as the vendor, the Appliance tab appears where you must specify the host that will perform the scan.

Instructions for configuring the in-network scanner host can be found on the Qualys website:

<https://www.qualys.com/docs/qualys-virtual-scanner-appliance-user-guide.pdf>

1. Select the Scanner Appliance.
2. Click **OK**.

Delete a vulnerability scanner

1. Select **System > Settings**.
2. Expand the **System Communication** folder.
3. Select **Vulnerability Scanners**.
4. Select the vulnerability scanner(s) you wish to delete, and click **Delete**.
5. A confirmation message is displayed. Click **Yes** to continue.

Admin FortiCloud SSO

Available in FortiNAC vF 7.6.3 +

Simplified single sign-on integration for FortiNAC administrative access that uses a pre-configured FortiCloud Identity Provider (IdP), requiring minimal setup. It allows administrators to authenticate into the FortiNAC GUI using their FortiCloud user credentials.

User account management is done within the Fortinet Customer Portal (not FortiNAC):

- Authorized users are FortiCloud user accounts. This could be the master user (email format) or IAM users
- IAM user creation and permissions are configured in the Fortinet Customer Portal (<https://support.fortinet.com>). Permissions are based upon the assets managed by the account.

For more information, see the [SAML SSO](#) integration.

CLI configuration

A CLI configuration is a set of commands that are normally used through the command line interface. The CLI configuration window allows you to create individual sets of commands, name them and then reuse them as needed to control ports, VLANs or host access to the network. When a CLI configuration is applied, the commands contained within it are sent to the selected network device. This modifies the network device's behavior as long as those commands are in force.

This software currently supports CLI commands for Cisco, D-Link, HP ProCurve, Nortel, Enterasys, Brocade, and Extreme wired and wireless devices. This document assumes that you are familiar with the CLI commands available for your devices and, therefore, does not include individual commands in the instructions.

It is recommended that you test all CLI commands or sets of commands using the console for the switch, router or other device before implementing CLI commands through FortiNAC. FortiNAC does not detect errors in the structure of the command set being applied on the device. CLI commands are applied to the device exactly as they are created.

You can create a set of CLI commands to perform an operation, and a separate set to undo the operation. Undo is triggered when FortiNAC recognizes that the host or device has disconnected from the port. The do and undo command combination is sometimes referred to as Flex-CLI. Note that by using both Set and Undo, the CLI configurations do not become cumulative on the device.

To access the CLI configuration view, go to **Network > CLI Configuration**.

Settings

Field	Definition
Name	Name used to identify the CLI configuration.
Description	User specified description for the CLI configuration.
Last Modified By	User name of the last user to modify the configuration.
Last Modified Date	Date and time of the last modification to this configuration.
Right click options	
Copy	Creates a copy of the selected CLI configuration.
Delete	Deletes the selected CLI configuration.
In Use	Provides a list of other features that reference this CLI configuration, such as a role mapping or a Scheduled Task. See Configuration in use on page 435 .
Modify	Opens the Modify CLI Configuration window. See Add or modify a configuration on page 436 .
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746

Field	Definition
	 You must have permission to view the admin auditing log. See Add an administrator profile on page 139.
Buttons	
Show CLI	Opens the CLI window and displays a all of the commands in the Set and Undo sections of the configuration. See Show configuration on page 435 .

There are several CLI Configuration events that can be enabled and mapped to alarms for notification:

Event	Definition
CLI Configuration Failure CLI Configuration Success	Generated when a user tries to configure a Scheduled task that involves applying a CLI configuration to a group. Indicates whether or not the configuration of the scheduled task was successful.
Host CLI Task Failure Host CLI Task Success	Indicates whether or not the CLI commands associated with host/adaptor based ACLs have been successful.
Port CLI Task Failure Port CLI Task Success	Indicates whether or not the CLI commands associated with port based ACLs have been successful.
Port CLI Data Substitution Failure Port CLI Data Substitution Success	Indicates success or failure to substitute the "Port, VLAN, IP, or MAC" data into the CLI.

Using CLI configurations you can do the following:

- Apply or remove specific CLI configurations to networking devices based on control states, such as registration, authentication, or quarantine. See [Apply a port based configuration via model configuration on page 440](#).
- Apply or remove ACL based CLI configurations to hosts connected to the network on a Layer 2 or Layer 3 device. The ACL modified by the CLI configuration controls host access to the network. These configurations can be applied or removed based on control states, such as registration, authentication, or quarantine. See [Apply a host based configuration via the model configuration on page 440](#) and [Requirements for ACL based configurations on page 446](#).
- Apply specific CLI configurations for roles. Note that roles are associated with device or port groups. Be sure to group devices with common CLI capabilities. See [Roles on page 620](#) and [Apply a CLI configuration using a role on page 441](#).
- Apply specific CLI configurations for network access policies. When using user/host profiles to determine Access Policies, use location criteria to group devices with common CLI capabilities. See [Network access on page 482](#) and [Apply a CLI configuration using a network access policy on page 445](#).
- Create a scheduled task for a CLI configuration to be applied to a device group. See [Apply a CLI configuration using a scheduled task on page 445](#).
- Use port logging capabilities to see which port control changes and CLI configurations were applied and when. See [Port changes on page 455](#).

Variable options

Substitution Data	Port Based DO	Port Based UNDO	Host Based DO	Host Based UNDO
%port%	Yes	Yes	Yes	No
%vlan%	Yes (if specified in network access configuration)	Yes (from present "current" vlan of the port)	Yes (from present "current" vlan of the port)	No
%ip%	No	No	Yes	Yes
%mac%	No	No	Yes	Yes

Configuration in use

To find the list of FortiNAC features that reference a CLI configuration, select the configuration from the **CLI Configurations** view and click **In Use**. A message is displayed indicating whether or not the configuration is associated with any other features. If the configuration is referenced elsewhere, a list of each feature that references the configuration is displayed.

Show configuration

This option displays a all of the commands within the CLI configuration.

1. Select **Network > CLI Configuration**.
2. Select the configuration and click **Show CLI** to display the commands within the configuration.



FortiNAC provides the proper login command sequence and final logout or exit commands. Your CLI should include exit commands to exit modes entered within the CLI. The final session logout or exit is done by FortiNAC.

Port based and host based configurations

Port based CLI configurations are used to switch VLANs for a host, modify port behavior for a host or to reconfigure settings on a group of switches. Host based CLI configurations are used in environments where you have many hosts connecting through a single port and those hosts need to be controlled individually instead of based on the least secure host.

Host based CLI configurations leverage the use of ACLs stored on a Layer 3 device by adding or removing IP addresses from the ACL.

Below is a list of devices and the types of CLI configurations supported.

Devices	Port Based	Host Based
Cisco	Yes	Yes

Devices	Port Based	Host Based
D-Link	Yes	Yes
Enterasys	Yes	Yes
Extreme	Yes	Yes
Brocade	Yes	Yes
HP ProCurve	Yes	Yes
Nortel	Yes	No

Add or modify a configuration



FortiNAC provides the proper login command sequence and final logout or exit commands. Do not include the login commands and logout or exit commands in the CLI.

1. Select **Network > CLI Configuration**.
2. To create a new CLI configuration, click **Add**.
3. To modify a CLI configuration, select it from the CLI configuration view and click **Modify**.
4. Right-click in any of the three main text areas for a pop-up menu with editing options: Undo, Cut, Copy, Paste, Delete, and Select All. You can also use Ctrl+x, Ctrl+c, and Ctrl+v to cut, copy, and paste.
5. Enter a name for the CLI configuration. This name displays in other parts of the software allowing you to choose and implement this configuration.
6. If you plan to use MAC address in your CLI configuration, select the **MAC Address Format** that is recognized by the device to which you are applying this configuration.
7. Click in the **Commands To Set** field and enter the CLI commands to be stored as a configuration.
8. If you would like to reverse those commands when the port state or host state changes, go to the **Commands To Undo** field and enter the appropriate commands. Use **Copy** to copy commands from Commands To Set to Commands To Undo.



In the event of a device failure or power cycle, changes made by CLI command sets to the device configuration could be lost. FortiNAC will not resend CLI command sets that were sent successfully. It is recommended that you include a command such as `write mem`, in the creation of your CLI command sets to ensure that the most recent configuration is saved on the device.

9. Enter a **Description** of the CLI configuration. This field is not required.
10. Click **OK** to save.

Settings

Field	Definition
Name	Required. Assign a descriptive name to the CLI command set.

Field	Definition
MAC address Format	If you choose to modify an ACL by adding or removing MAC addresses, you must select the MAC address format that is recognized by your device. If this format is incorrect, the device will not be able to interpret the MAC address information in the ACL.
Commands To Set	Required. Enter the commands that comprise the configuration. Following is an example: <pre> config t interface %port% speed 10 duplex half exit exit </pre> You can use shorthand if it is supported on your networking device. The commands you enter in the CLI configuration window dynamically populate port/interface, VLAN IDs, IP addresses and MAC addresses based on your choice of CLI control mechanism. Each variable in the CLI configuration is treated as a separate entity. You can use the variables any number of times or not at all, based on your choice of CLI commands.
%port% %vlan%	%port% and %vlan% for the Commands to Set and Commands to Undo text areas simplify adding this substitution parameter.
%ip%	%ip% allows you to quickly add this parameter into the CLI configuration and can be used to add or remove IP addresses from an ACL. Can be used only on Layer 3 devices such as routers.
%mac%	%mac% allows you to quickly add this parameter into the CLI configuration and can be used to add or remove MAC addresses from an ACL. When you click this button it also inserts the MAC address format selected at the top of the window. Can be used only on Layer 2 devices.
Copy to Undo	Click this button to copy the commands from the Commands to Set pane to the Commands to Undo pane. Edit the commands in this pane to add a negate command.
Commands To Undo	Optional. This field allows you to reverse commands in the Commands To Set field. For example, if you change speed or duplex on a port for a host, you may need to return that configuration to its default setting when a different host connects. Example: <pre> config t interface %port% speed auto duplex auto exit exit </pre>
CLI Description	Detailed description of the command set for reference and clarification.

Sample configurations

The port- and host-based CLI configurations shown below are samples of different types of configurations that may help you develop your own.

Example 1: Port based configuration - port speed

The configuration shown below modifies the speed and duplex configuration of the port and then returns it to its normal state.

Commands	CLI configuration
Set	<pre>config t interface %port% speed 10 duplex half exit exit</pre>
Undo	<pre>config t interface %port% speed auto duplex auto exit exit</pre>

Example 2: Host based CLI configuration - IP address

The configuration shown below modifies an IP address ACL on the device to switch access for the host's IP address from the FortiNAC software DNS server to the production DNS server. When the host is restricted to the FortiNAC software DNS server, it is essentially in isolation and can be forced to register. When the host has access to the production DNS server, it can connect to the network and access the Internet.

Commands	CLI configuration
Set	<pre>config t ip access-list extended Nac 1 deny udp host %ip% host 192.168.34.2 eq domain 2 permit ip host %ip% host 192.168.105.2 exit ip access-list resequence Nac 10 1 end write mem</pre>
Undo	<pre>config t ip access-list extended Nac no deny udp host %ip% host 192.168.34.2 eq domain no permit ip host %ip% host 192.168.105.2 end write mem</pre>

In the example above 192.168.34.2 is the production DNS server and 192.168.105.2 is the FortiNAC software DNS server. In the second line, Nac is the name of the ACL. ACL name is case sensitive. If the name is not correct, the ACL is not modified.

The `ip access-list resequence Nac 10 1` command is important because it controls the sequence in which the host IP addresses are entered into the ACL. Starting with line 10, each IP address is added to the beginning of the list. Addresses already in the list are incremented by one.

If FortiNAC cannot determine the IP or any data substitution value of the host, the CLI will not be run. A CLI Substitution Failure Event is generated describing the data which could not be substituted.

Example 3: Host based CLI configuration - MAC address

The configuration shown below modifies a MAC filtering ACL on the device to deny access to a particular MAC address sent by FortiNAC.

Commands	CLI configuration
Set	<pre> config t mac access-list extended Nac 1 deny %macXXXX.XXXX.XXXX% any exit mac access-list resequence Nac 10 1 end write mem </pre>
Undo	<pre> config t mac access-list extended Nac no deny %macXXXX.XXXX.XXXX% any end write mem </pre>

In the example above, Nac is the name of the ACL. ACL name is case sensitive. If the name is not correct, the ACL is not modified.

The `mac access-list resequence Nac 10 1` command is important because it controls the sequence in which the host MAC addresses are entered into the ACL. Starting with line 10, each MAC address is added to the beginning of the list. Addresses already in the list are incremented by one.

Implement configurations

CLI configurations can be implemented on the device itself to control network access based on host state using model configuration. They can also be associated with a role or a network access policy. Devices that connect to devices or ports with that role trigger the application of the CLI configuration. Hosts that connect to devices or ports associated with the network access policy trigger the application of the CLI configuration. CLI configurations can be applied to device or port groups based on a scheduled task.

When a CLI configuration has been applied based on one of the criteria listed above, it remains in effect until something else happens. For example, if a CLI configuration is applied based on a network access policy, when the host connects to a port and both the host and the port are included in the policy, the associated CLI configuration is applied. The CLI configuration remains applied to the port until a different CLI configuration is applied or the UNDO commands are triggered. A host disconnect or a VLAN change will trigger the UNDO.

Apply a port based configuration via model configuration

When hosts connect to the network, the FortiNAC software determines the host's state. Based on that state the host may be sent to registration, quarantine, authentication, dead end, or the production network. The configuration of the device to which the host has connected controls the host's network access.

Use model configuration of your FortiNAC software to set just a VLAN for each host state, a VLAN and a CLI configuration for any of those states or nothing. If you set a CLI configuration for a state, you must also set a VLAN for that state even if it is just the production VLAN. When both a VLAN and a CLI configuration are set for a particular host state, they can work in conjunction with each other. For example, if authentication is set to VLAN 10 and a CLI configuration is also applied, that configuration might reduce bandwidth while the user is in the authentication VLAN.

CLI configurations will not be applied if there is no VLAN selected in the **Network Access** section of the model configuration.

This option is used when you would like to apply a CLI configuration to hosts who do not match a network access policy. Typically these hosts would not have a policy because they have not registered or been authenticated and the FortiNAC software does not know who they are.

1. Select **Network > Inventory**.
2. Right-click on the device and then click **Model Configuration**.
3. In **General**, enter the **User Name** and **Password** for CLI access to the device.
4. In **Protocol**, select the communication protocol for this device.
5. In **Network Access**, select **Read VLANs** to populate drop-downs for each host state. Select the VLANs used for each host state. Note that you should not fill in the Default field if ports on this device have different default VLAN settings. Default VLANs should be set in **Network Access/VLANS**. If all ports on the device use the same default VLAN, you can set it here.
6. In the **CLI Configurations** section, select the type as **Port based**. Port based configurations affect the port directly.
7. Select a **CLI Configuration** for the host states you wish to affect.
8. If you are using a RADIUS server for authentication, the default servers are displayed and do not need to be modified. If this device should use a different RADIUS server for authentication, select it from the drop-down list and enter the matching RADIUS Secret.
9. Click **Apply** to save your changes.

Apply a host based configuration via the model configuration

Host-based CLI configurations modify ACLs stored on the switch or router. CLI configurations that modify IP address ACLs can only be used on Layer 3 devices.

or removes IP addresses from a corresponding ACL based on the host state. When the host connects, the FortiNAC software determines whether or not they need to be sent to registration, authentication, remediation or remain in a dead end. When the host has satisfied the requirements of its state and is ready to be put on the production network, the state change triggers the undo portion of the CLI configuration updates the ACL again. This allows the host onto the production network.

1. Select **Network > Inventory**.
2. Right-click on the device and then click **Model Configuration**.
3. In **General**, enter the User Name and Password for CLI access to the device.
4. In **Protocol**, select the communication protocol for this device.

5. In **Network Access**, select **Read VLANs** to populate the VLAN drop-downs. Set the VLANs used for each host state. Note that you should not fill in the Default field if ports on this device have different default VLAN settings. Default VLANs should be set in **Network Access/VLANs**. If all ports on the device use the same default VLAN you can set it here.
6. In the **CLI Configurations** section, select the type - **Host Based**. Host based configurations control host access through the use of an ACL stored on the device and referenced in the CLI configuration.
7. Select a CLI configuration for the host states you wish to affect. If you select a CLI configuration you must set a corresponding VLAN.



Right-click the device and select the **Applied ACLs** menu option to view or clear applied ACL settings. The Applied ACL menu option is available after a Host Based Configuration is applied. You may need to refresh the Inventory.

8. If you are using a RADIUS server for authentication, the default servers are displayed and do not need to be modified. If this device should use a different RADIUS server for authentication, select it from the drop-down list and enter the matching RADIUS Secret.
9. Click **Apply** to save your changes.

View/clear applied ACL settings

If you have applied host based CLI configurations, you may want to see and/or remove changes to the ACL on the device. This option is accessed via the Applied ACL window.

1. Select **Network > Inventory**.
2. Expand the **Container** holding the device.
3. Right-click on the device. Select the device name and then click **Applied ACLs**.



The Applied ACL menu option is available after a Host Based Configuration is applied. You may need to refresh the Inventory.

The Applied ACLs window opens, displaying the name, MAC address, IP address, CLI, and Host for each Applied ACL.

4. Select the ACL(s) you wish to delete, and then click **Delete**. If there is an Undo configuration, it will be run.
5. Click **Close** to exit.

Apply a CLI configuration using a role

CLI configurations applied based on a role are typically port based not host based. It is not recommended that you use host based CLI configurations with roles.

Network device roles allow you to control network access based on combinations of devices and connection locations. Each role that is created can be applied to individual devices.

Devices that require network services can only have one role. Switches or ports to which devices connect for network access can be mapped to more than one role. The role mapping provides the switches and ports with rules when something with a matching role connects.

To provide more flexible control using roles you can apply a CLI configuration instead of just switching VLANs.

Refer to [Assigning roles on page 621](#) to set roles for hosts, network devices and ports. Then refer to for step-by-step instructions.

Role assignments

Roles can be assigned to users, hosts, network devices and ports. Each one of these entities has a role field on its corresponding **Properties** window. Assignment of roles is accomplished by setting the role field for the user, host, device or port either manually or using one of the options listed in the table.



When a user and a host have different roles, the user role is applied if the user logs into the host. In the case of a gaming device that the user does not log into, it has its own role that may or may not be the same as the user's.

In the event that multiple methods are used to set a role, the order of precedence is determined by the order of the roles on the **Roles** view. Starting from the top of the list, the first role match found is used. For example, assume you have assigned roles to hosts based on groups. Later you add the host to a new group, if that group is associated with a role that is ranked above the host's original role, the host's role will be changed.

In the event that multiple methods are used to assign a role to a host, a hierarchy determines which role to assign. Roles assigned through Portal pages (typically for gaming), have the lowest precedence and will be overwritten by a role determined by any other method. Roles assigned by directory attributes have the highest precedence and will overwrite a role that is assigned by any other method. Roles assigned by group membership have the middle level of precedence, overwriting roles assigned through Portal Pages, but being overwritten by roles assigned via directory attributes. Roles assigned via group membership will change when the host's group membership changes. When this occurs, the roles are ranked, with low-numbered ranks having the highest precedence.

Roles	Definition
User roles	
User Roles Based On Groups	Users can be assigned roles by placing them in a group and then associating that group with a role on the Role View. See Add a role on page 626 for additional information on adding roles. Once the group of users has been created and you have assigned them a role, you must associate that role with a device group or a port group and a corresponding VLAN or CLI configuration. User groups can also be created based on groups in the directory. These groups are treated the same as groups created manually within FortiNAC. If a user is a member of more than one group the group that is found first when matching users to roles determines the role assigned to the user.
	 When assigning Roles to users, the use of directory attributes over directory groups is recommended. Attribute data is retrieved directly from the directory as the user registers, while group information is retrieved from data cached on the FortiNAC server and could be out-dated.

Roles	Definition
User Roles Based On A Directory Field	Network users can be assigned a role based on a field in LDAP or Active Directory. For example, you might choose to have roles based on a field in the directory called Department. The data within the Department field would be the name of the role, such as Accounting or Customer Service. In a university environment a user might have a role based on whether he is a Student or Faculty. To assign roles based on a field in a directory you must indicate which field in the directory is to be used as a role. See to map the role field. Users in the directory with matching data in this field constitute a group, even though the group is not shown anywhere. For example, users with Accounting in their department field are treated as an Accounting group for the purpose of assigning roles. Next, you must create a Role with the exact same name as the data contained in the directory field. For example, if the user's role in the directory is Accounting, you must create a Role on the Role View that is named Accounting. When a user registers, the role field in User Properties is set to match the data in that user's role field in the directory.
User Roles Based On Fields In Captive Portal	When registering a host through the Captive Portal, if the user fields on the portal page have a role set, that role is assigned to the user, such as during registration or authentication.
Individual User Roles	In some situations you may want to assign a role to a single user. First create the role on the Roles view. Then, navigate to the User Properties window and modify the Role field.
Host roles	
Host Roles Inherited From Users	When registering a rogue to a user on the Host View, you have the option to use the user's role or to select a different role for the device. See Add or modify a host on page 227. When registering a host through the Captive Portal, if the portal does not have a role set, the host inherits the role of the user. If the users role changes, regardless of how it is changed, any host registered to that user that has the same role will be changed also. Example: John Doe is a student and has two registered hosts. John Doe's Role: Student John Doe's Host 1 Role: Student John Doe's Host 2 Role: Gaming John Doe graduates and becomes faculty, so the University makes the change in AD and runs a directory sync. John's role is changed to Faculty. John Doe's Role: Faculty John Doe's Host 1 Role: Faculty John Doe's Host 2 Role: Gaming Host 2 did not match John's original role of Student, so it is not changed.

Roles	Definition
Host Roles Assigned Through Captive Portal	When registering a host through the Captive Portal, if the portal page has a role set, that role is assigned to the host during registration. If the role field is blank, the host inherits the role of the user.
Host Roles Based On Groups	Hosts can be assigned roles by placing them in a group and then associating that group with a role on the Roles view. See Add a role on page 626 for additional information on adding roles.
Host Roles Assigned Manually	This would typically be used to assign a role to hosts, such as a medical device that connects to the network. To register rogues and set their role: 1. Select one or more rogues on the Host View. 2. Right-click on the selected records and choose Register as Device from the menu. 3. On the registration pop-up, select device type and role. See Register a host as a device on page 232. To set roles for registered devices: 1. Select one or more devices on the Host View. 2. Right-click on the selected records and choose Set Host Role. 3. Select the new role from the drop-down list in the pop-up window.
Host Roles Assigned By Device Profiler	This would typically be used to assign a role to hosts, such as a medical device that connects to the network. Devices that are hosts, such as medical devices, gaming devices, or printers can be assigned a role and a device type based on device profiling rules. If you are using the device profiler feature, you can create or use default rules that allow FortiNAC to determine the device type and assign the device to a role. When a new host device connects to the network it becomes a rogue because it is unknown. FortiNAC compares information received from the device with the device profiling rules in its database until it comes up with a match. Based on the parameters defined in the rule, the device is assigned a type and a role. See Profiled devices on page 251 and Device profiling rules on page 259. The role assigned by device profiler takes precedence over any role associated with the vendor OUI.

Configure a role with CLI

1. Select **Policy & Objects > Roles**.
2. Click **Add**.
3. In the **Name** field, enter a name for the new role.
4. Click **Select** next to the Groups field. Choose one or more groups by clicking on the names in the **All Groups** column and clicking the right arrow to move them to the **Selected Groups** column. Click **OK** to continue.
5. Click in the **Note** field to add any user defined information needed for this role.
6. Click **OK** to save the role.
7. Click on **Network Device Roles** in the menu to create a mapping for this role.
8. Click **Add** at the bottom of the screen.

9. Click the **Role** check box to enable the role drop-down. If this is not enabled, this mapping can apply to any device that matches the other criteria in the mapping, such as Location. The word Any displays in the Role column on the network device roles view if this box is unchecked.
10. Select the role you created earlier from the drop-down list.
11. If applicable, in the **Access Value** field type the network access identifier for this mapping, such as a VLAN ID, VLAN Name, Aruba Role or for a VPN concentrator enter a group policy name.
12. Click **Select** next to the Location field. Choose one or more device or port groups by clicking on the names in the **All Groups** column and clicking the right arrow to move them to the **Selected Groups** column. Click **OK** to continue.
13. Click in the **Note** field to add any user defined information needed for this mapping.
14. Click **OK** to save the mapping.

Apply a CLI configuration using a network access policy

CLI configurations applied based on a network access policy are by default port-based not host based.

Network access policies use user/host profiles to match a host with a network access configuration. Network access configurations contain VLAN and/or CLI configuration information. Each user/host profile used to apply a CLI configuration should contain the group of devices or ports to which the host must be connected and the rules or filters that determine whether or not the network access configuration should apply to the connecting host. The groups of devices or ports should contain devices that can accept CLI configurations.

To provide more flexible control using network access policies you can apply a CLI configuration instead of just switching VLANs.

Refer to [Network access on page 482](#) to set policies for hosts, network devices and ports.

1. Select **Policy & Objects**.
2. Select **Network Access**.
3. Click **Add** or select an existing Policy and click **Modify**.
4. Click in the **Name** field and enter a name for this policy.
5. Click the **Add** icon next to **User/Host Profile**. Only certain devices can accept CLI configurations. At minimum you must configure the Where field for the user/host profile to ensure that CLI configurations are applied only to devices that can accept them. The remainder of the user/host profile can be configured any way you wish. Click **OK** to save the profile. Connecting users/hosts must match this user/host profile to be assigned the network access configuration specified in the next step.
6. Click the **Add** icon next to **Network Access Configuration**.
7. Enter the name for the configuration, then choose an existing logical network, or click **Create** to create a new logical network. Click **OK** to save the network access configuration. See [Create or edit a configuration on page 487](#) for additional information.
8. The **Note** field is optional.
9. Click **OK** to save your Policy.

Apply a CLI configuration using a scheduled task

This option is typically used when configuring a group of devices that can interpret the same set of CLI commands. For example, if you are configuring devices to send traps back to your FortiNAC software, you can apply a CLI configuration using a scheduled task to configure them all at once instead of logging into each device individually.

1. Go to **System > Scheduler**.
2. Select **Add**.
3. Enter a **Name** for the task and an optional description.
4. In the **Action Type** field select CLI. CLI actions are sets of command line instructions that are created in the CLI configuration view and saved to be executed elsewhere in the program.
5. Select the **Action** from the list of CLI actions.
6. From the **Select a Group** drop-down list, select the group of devices to which the CLI configuration will be applied.
7. From the **Schedule Type** drop-down select either **Fixed Day** or **Repetitive** and set the day and time that the task is to be performed.
8. A **Fixed Day Task** is one that you can schedule to run any day at any time. Selects the day(s) and time to run the task.
 - a. Click the box next to the day(s) to select the day.
 - b. Click the down arrows and select the hour, minutes, and AM or PM from the drop-down list for each day.
 - c. To enter days/times more quickly, select **Set Multiple Days** to set multiple days with the same time.
 - d. To remove all settings, select **Clear All**.
9. A **Repetitive Task** is one you configure to run on a given day, at a specific time for a specified number of repetitions. The repetition rate can be set to any number of minutes, hours, or days.
 - a. Enter the **Repetition Rate** using whole numbers.



A repetition rate of zero causes the task to run only once.

- b. Click the down arrow and select Minutes, Hours, or Days from the drop-down list.
 - c. Enter the date and time for the task to run in the **Next Scheduled Time** field using the format MM/DD/YY hh:mm AM/PM Time Zone.
 - d. Click **Update** to update the **Next Scheduled Time** field or change the **Repetition Rate**.
-



The new Repetition Rate does not take effect immediately. It starts the next time the scheduled task runs. For the new Repetition Rate to take effect immediately, select **Update**.

10. Click **OK**.

Requirements for ACL based configurations

CLI configurations can be created in your FortiNAC software to modify ACLs based on host state. These CLI configurations are applied via model configuration for the device that contains the ACLs. See [Apply a host based configuration via the model configuration on page 440](#). This section provides an overview of the basic setup required within FortiNAC along with some sample ACLs and CLI configurations.

Requirements For IP ACL based configurations

- Devices to which these IP address based CLI configurations are applied must be Layer 3 devices, such as a router or a Layer 3 switch.

- VLAN Switching and MAC Filtering must be disabled for the device. To disable these options locate the device in the Inventory. Right-click and select Properties.
- Switches connected to Layer 3 devices should not be modeled in FortiNAC.
- In order to control access to the production network, the ACL permits or denies access to either the FortiNAC DNS server or your regular DNS servers. By doing this the host retains the same IP address throughout the transition to the production network. Therefore, the DHCP server for your hosts should be your regular DHCP server and not FortiNAC.
- Since hosts are switched to the FortiNAC DNS server during isolation, you must add the FortiNAC IP address to the Production DHCP's list of DNS servers.
- Make sure that the lease pool and lease times are large enough that hosts always receive the same IP address. If a host's IP address changes before the registration process is complete, then the ACL is not updated correctly.
- The host's browser caches the registration page. After a host has successfully registered, the success page tells the host to close the browser. If you are using the Dissolvable Agent, the Renew IP option must be enabled. This forces the IP address to be released and clears the cache.

Create the Cisco extended ACL

An extended ACL is an ordered list of statements that can deny or permit packets based on source and destination IP address, port numbers and upper-layer protocols.

This ACL is a sample of the type of ACL you might create to work in conjunction with your FortiNAC software and its CLI configurations. Be sure that you know the IP address of the FortiNAC appliance and the IP range of the DHCP scope for your hosts. Log into the device and create an extended access list.



All information in an ACL is case sensitive.

Example

```
Configure term
ip access-list extended Nac
500 permit tcp 192.168.34.0 0.0.0.255 host 192.168.105.2 eq 4568
501 deny ip 192.168.34.0 0.0.0.255 host 192.168.105.2
502 permit ip any any
end
write memory
```

Settings

Command	Definition	Data From Example
ip access list extended	Indicates the type of ACL and the user specified name of the ACL. In this example, the name is Nac.	ip access list extended Nac
permit or deny	Allow or block traffic. This is a required field.	
protocol	IP, TCP, UDP, ICMP, GRE and IGRP. TCP, UDP and ICMP use IP at the network layer.	udp ip

Command	Definition	Data From Example
source	This is the Source IP address. This is a required field. In the example, this is the IP range for your hosts. When <any> is used it indicates that any IP address can connect.	192.168.34.0 any
source mask	Wildcard mask; 0 indicate positions that must match, 1s indicate don't care positions (inverted mask). Required.	0.0.0.255
destination	Destination IP address. This is the IP address of the FortiNAC appliance that is used for isolating hosts who are not registered or who have failed a security policy scan. When <any> is used it indicates that the host can connect to any IP address.	host 192.168.105.2 any
operator destination port	lt, gt, eq, neq (less than, greater than, equal, not equal) and a port number. In this example 4568 is the port number through which the Persistent Agent communicates with the FortiNAC appliance. This must remain available if you are using the Persistent Agent to scan your hosts.	eq 4568

In the example 192.168.34.0/24 is the hosts IP range. The host IP 192.168.105.2 is the Isolation interface on the FortiNAC appliance. This is the default state of the all registered hosts. It allows the hosts to go to anywhere on the network except the Isolation interface.

Apply the ACL to the physical interface

Once you have created one or more ACLs you must apply them to the port or ports on the device where the edge switches connect. These ports will be controlled by the ACL based on the host state. Below is an example of the command needed to apply the ACL. This may vary depending on the device.

```
Configure term
interface FastEthernet1/0/11
ip access-group Nac in
```

```
end
write mem
```

Poll the switch/router

In order for FortiNAC to monitor the hosts connected to the device, it must poll the device periodically. Polling is set up automatically as devices are added to FortiNAC.

As devices are added they are evaluated. Any device that is capable of L2 polling (polling hosts) is immediately placed in either the L2 Wired Devices or L2 Wireless Devices sub-group. These are default groups that are created in the database and populated for you. The default polling interval is 10 minutes for wireless devices and one hour for wired devices.

To modify polling intervals select **Network > L2 Polling**. See [L2 polling on page 449](#) for additional information.

L2 polling

L2 Polling is one in a series of initial setup windows designed to help you get your FortiNAC program up and running as quickly as possible. Similar functions exist in other parts of the software, but this window provides access to the most essential configuration information.

The L2 polling function is used by FortiNAC to learn where hosts are connected on the network based upon their MAC address. FortiNAC reads the network device's MAC Address table. The database is updated with the MAC address, corresponding switch and port location. For other methods used for tracking hosts, see [Learning about hosts on the network](#).

L2 polls are triggered by the following:

- L2 polling interval as defined for the device model (wired devices default: 60 minutes, wireless devices default: 10 minutes)
- Manually - see [Poll for L2 \(hosts\) information](#).
- Receipt of SNMP Link Up trap (If no MAC entry found in table, will attempt 3 more times)
- Receipt of a mac-notification trap if no port can be identified from the trap info.

The L2 Polling window displays devices that were added either manually or through Discovery on the Network Devices window. As devices are added they are evaluated. Any device that is capable of L2 polling (polling hosts) is immediately placed in either the L2 Wired Devices or L2 Wireless Devices sub-group. These are default groups that are created in the database and populated for you. Devices that are not in one of these groups do not display on the L2 Network Devices window.

L2 Network Devices listed here are configured to poll network hosts and discover their IP addresses. The default polling interval is 10 minutes for wireless devices and one hour for wired devices. Devices displayed here can be added to or removed from the L2 Network Device Groups and their polling settings can be modified.

To access click **Network > L2 Polling**.

Settings

Fields used in filters are also defined in this table.

Field	Definition
Name	Name of the selected device.
#	Indicates the order of display.
Type	Indicates the type of devices, such as switch, printer, router, etc.
IP address	IP address of the selected device. IP addresses or Address Ranges are used to add or discover devices.
Status	Indicates whether or not communication has been established with the device. Displays either Established or Lost.
Groups	Indicates that the device is a member of the groups listed.

Field	Definition
Views	Series of icons that can be clicked to provide additional details about the selected device. Icons provide access to Device Properties, group membership and Ports and Hosts. Click an icon to access the view.
L2 Polling	Indicates whether or not L2 polling is enabled and the time interval between polls.
L2 Last Polled	Date and time of the last polling attempt, regardless of whether it was successful or not.
L2 Last Poll Success	Date and time of the last successful poll.
Container	Container in the Inventory where the device is stored. Containers are a grouping mechanism similar to folders.
Right click options	
Export	Exports data to a file in the default downloads location. File types include CSV, Excel, PDF, or RTF. See Export data on page 116 .
Add To Group	Adds selected devices to a user specified device group.
Remove From Group	Removes selected devices from a user specified group.
Set Polling	Allows you to enable or disable polling and set the polling time interval for the selected device(s).
Poll Now	Polls selected devices immediately instead of waiting for the next poll interval.

Set L2 polling

1. Click **Network > L2 Polling**.
2. The L2 Network Devices window displays.
3. Select one or more devices from the list. To select all devices, click **Select All**.
4. Click **Set Polling**.
5. Use the **Enable Polling** check box to enable or disable polling for the selected device.
6. If polling is enabled, select a time interval to control how often polling should occur. The interval can be set in Hours or Minutes.
7. Click **OK**.

L3 polling

L3 Polling is one in a series of initial setup windows designed to help you get your FortiNAC program up and running as quickly as possible. Similar functions exist in other parts of the software, but this window provides access to the most essential configuration information.

L3 Polling triggers the IP address to MAC address conversion. Based on the information returned, FortiNAC resolves the MAC addresses associated with IP addresses for hosts and other devices on the network.

L3 devices are polled based on the following:

- L3 polling interval as defined for the device model
- Whether a host is being evaluated by a device profiling rule that requires IP address information. Device Profiler will attempt to find an up-to-date IP address for a particular host for 30 minutes before giving up if an up-to-date IP address cannot be found.
- (as of 9.1) A VLAN change has occurred. The system performs the below steps to update the affected host's IP information:
 1. Waits 20 seconds after VLAN change
 2. Looks in the internal cache for an IP change due to either a Persistent Agent update or scheduled L3 poll.
 3. If IP has not changed, the system polls the last L3 device that had an entry for the host's MAC address. If no entry is found, the host location's next hop router is polled.
 4. If no new IP address is found, the system waits 30 seconds.
 5. If no new IP address is found, steps 3 and 4 are repeated 4 more times.

Use this window to set a polling interval for switches and routers.

As devices are added or discovered they are automatically added into the L2 Network Devices group and either the L2 Wired Devices or L2 Wireless Devices sub-groups. A default L3 (IP --> MAC) group is created by FortiNAC but is not automatically populated. You must add your L3 devices to this group.

By default this window displays devices that have been manually placed in the L3 (IP --> MAC) group. If you have not placed any devices in this group, the window does not display any devices. Select the All Devices option and click **Refresh** to display all network devices in the window.

To access click **Network > L3 Polling**.

Settings

Fields used in filters are also defined in this table.

Field	Definition
Display	All Devices: Displays all network devices. When Group is selected in the Filter By section, all device groups are displayed in the Group drop-down. L3 (IP --> MAC) Devices: Displays all devices in the L3 (IP --> MAC) Devices group. When Group is selected in the Filter By section, the L3 Devices group and any sub-groups are displayed in the Group drop-down.
#	Indicates the order of display.

Field	Definition
Name	Name of the selected device.
IP address	IP address of the selected device. IP addresses or Address Ranges are used to add or discover devices.
Type	Indicate the type of devices, such as switch, printer, router, etc.
Status	Indicates whether or not communication has been established with the device. Displays either Established or Lost.
Groups	Indicates that the device is a member of the groups listed.
Views	Series of icons that can be clicked to provide additional details about the selected device. Icons provide access to Device Properties, group membership and Ports and Hosts. Click an icon to access the view.
L3 Polling	Indicates whether or not L3 polling is enabled and the time interval between polls.
L3 Priority	Indicates high, medium or low priority given to the device when hosts connect to the network. Devices are polled in batches based on priority to retrieve host IP addresses. It is recommended that high traffic routers and switches be given a higher priority to allow hosts on those devices to connect more quickly.
L3 Last Polled	Date and time of the last polling attempt, regardless of whether it was successful or not.
L3 Last Poll Success	Date and time of the last successful poll.
Container	Container in the Inventory where the device is stored. Containers are a grouping mechanism similar to folders.
Export	Exports data to a file in the default downloads location. File types include CSV, Excel, PDF, or RTF. See Export data on page 116 .
Right click options	
Add To Group	Adds selected devices to a user specified device group.
Remove From Group	Removes selected devices from a user specified group.
Set Polling	Allows you to enable or disable polling and set the polling time interval for the selected device(s).
Poll Now	Polls selected devices immediately instead of waiting for the next poll interval.

Set L3 polling

L3 devices have a Priority setting that allows you to associate a High, Medium or Low polling priority with each L3 device. When hosts connect to an L3 device the priority setting determines how quickly the device is polled. For example, if you have a high traffic device and a low traffic device and hosts are seen on both, which should be polled first? Typically you would give the high traffic device a high priority and the low traffic device a low or medium priority. When hosts are seen by both devices, the high priority device would be polled first. If you expand this example throughout your network, devices will be polled in groups by their priority with high priority devices being polled first.

1. Click **Network > L3 Polling**.
2. The Devices window displays.
3. Select one or more devices from the list. To select all devices, click **Select All**.
4. Click **Set Polling**.
5. Use the **Enable Polling** check box to enable or disable polling for the selected device.
6. If polling is enabled, select a time interval to control how often polling should occur. The interval can be set in Hours or Minutes.
7. In the **Priority** field, select the priority given to the device when hosts connect to the network. The higher the priority the more quickly a host connects.
8. Click **OK**.

L3 Device Identification

This is a process that reads from configured Network Devices and attempts to determine if they support L3 routing. For each device, a Score is computed on a range of 0 to 100 of the likelihood that the device supports L3. Once the scan of all devices is complete, the results may be viewed using the **L3 Identification Results** task. If the Score is at least 66, FortiNAC will suggest adding to the L3 group. If the Score is less than 33, FortiNAC will suggest removing from the L3 group. A selection to include in the L3 group must be made for each device before the changes may be saved.

The scan may be started from either the **Network > Inventory** view or the **Network > L3 Polling** view by clicking **"Start L3 Identification."**

Network events

The Network Events view displays the contents of the connection log: a list of historical host/user network events.

When the total number of records from Port Changes and Network Events views exceeds 100K, the oldest 20K entries (Port Changes and/or Network Events) are archived. Table size is not modifiable.

To access the Network Events view, select **Network > Network events**.

Filter/Configure Column

Each column header has a filter option. To filter:

1. Hover over the column header to reveal the filter icon.
2. Click the icon.
3. Set desired filter criteria.
4. Click **Apply**.

Settings

Field	Definition
Timestamp	Date/time of the logged event
Event Type	Name of the event (adapter connected, adapter disconnected, etc.).

Field	Definition
IP Address	IP address of the device that made the connection.
MAC Address	MAC address of the host or device that made the connection.
Type	Indicates whether the host is Registered or a Rogue.
Location	Current or last known location of the device that made the connection.
Logical Network	Name of the Logical Network applied when a policy is enforced (Event Type column displays "Applied Role/Policy").
Net ID	Used to store data such as vlanID, vlanName, whatever relevant info we may have access to (will vary based on event).
CLI Config Name	Name of CLI Configuration used (if any).
Radius	Flag to indicate if event is Radius or not.
Radius Attribute Default Group	Empty if not radius, otherwise shows the Attribute Default Group name.
Radius Attribute Logical Network Group	Empty if not radius, otherwise shows the Logical Network Group name.
Buttons	
Details	Shows verbose debug information for Network Events if enabled via the global options table. To enable, add an option with a key "networkSession.captureSnapshots" and a value "true".
Network sessions	Shows information of associated Network Sessions (previously Fortigate Sessions).
Toggle	
Filter Child Records	If enabled, this toggle will apply configured column filters to all child records as well as parent records.

Port changes

When the port's VLAN changes, a port-based CLI configuration is applied or RADIUS Access Accept is received, entries are written to the Port Changes view.

When the total number of records from Port Changes and Network Events views exceeds 100K, the oldest 20K entries (Port Changes and/or Network Events) are archived. Table size is not modifiable.

Settings

Fields used in filters are also defined in this table.

Field	Definition
Port changes	
Date	Date that the change occurred.
CLI Config Name	CLI configuration used to modify the port state.
Port Change Reason	Reasons for changes in port state. Reasons include: • Registration: Port was moved into the registration VLAN. • Remediation: Port was moved into the remediation VLAN. • Dead End: Port was moved into the dead end VLAN. • Default: Port was moved to the default VLAN • Role: Port was moved into the VLAN specified by the role associated with the end-station and the port. • Authentication: Port was moved into the authentication VLAN. • Undo: Port was changed based on Undo commands in a CLI configuration. • RADIUS Accept: Port changed due to FortiNAC responding to a RADIUS Access Request with an Accept.
Role/Access Policy	Name of the Network Device Role or the network access policy that triggered the port change. Not all port changes are associated with a role or a policy.
Port	Port that was changed. Includes device name and port number.
VLAN	ID or Name of the VLAN where the port was moved.
Device	Filters results by the device where the affected ports reside. Use Sort By to resort devices in the drop-down list by name or by IP address.
Buttons	
Export	Exports data to a file in the default downloads location. File types include CSV, Excel, PDF, or RTF. See Export data on page 116 .
Show CLI Button	Displays the commands within the CLI configuration selected in the CLI Config Name column.

Access port changes view

1. Select **Network > Port Changes**.
2. In the **Port Changes** window, use the filter options to select the appropriate group of records.
3. To see the actual CLI configuration that was applied, select **Show CLI**. As you hover over CLI configurations in the **Port Changes** view, the contents are displayed in the **Show CLI** view.

Policy & Objects

Policies are assigned to hosts based on the user/host profile associated with each policy. User/host profiles allow you to select one or more pieces of user or host data to match with users and hosts and determine which policy is applied to that host. Policies are ranked in priority starting with number 1. When a host requires a particular service, such as network access, the host and user data are compared to the user/host profile in each policy starting with the first policy in the list. If the host and user do not match criteria in the first policy, the next one is checked until a match is found.

Types of data used to determine whether or not the host/user is a match include the following:

Data	Definition
Who/What	Attributes A host or user must meet all parameters within a single filter, but is only required to match one filter in the list. The attribute must be known at the time of connection. See Filter example on page 468. Note: Adapter status (Adapter -> Connected -> Online/Offline) should not be used for Network Access Policies. Adapter status changes as part of the authentication process and at the time of RADIUS authentication (FNAC post-auth processing), the adapter status will always be offline. RADIUS Attributes Used to match against endpoints pre- and post-authentication. Groups - Any — Matches any group. - Any Of — Matches any of the listed groups. Does not have to match everything, but has to match at least one group that has been selected. - All Of — Has to match every group that's been selected. - None Of — Has to match no group that's been selected.
Where	One or more port or device groups. A user/host profile can include more than one port or device group; however the connection location only needs to be contained in one of the selected groups. If the Where field is empty it is set to Any, indicating that location is not being used as criteria for the match, therefore any host connection location would be a match.
When	Allows you to create matches based on the current time. If Always is selected, then time of day is not used. If Specify Time is selected, then the current time must be within the days and times included in the list to be a match for the host.

The host/user must match at least one item in each field that contains criteria other than Any. If the host/user does not match something in all fields, the policy is not selected and the next policy is checked.

A host that has had a policy applied based on time of day, may be moved to a different policy when the window of time in the current policy has passed. For example, the host may be moved to another VLAN or disconnected from the network when the window of time in the applied endpoint compliance policy has passed. Hosts are re-evaluated frequently, such as when the device where they are connected is polled or when the Persistent Agent contacts the

server. If another Policy exists that applies to this host, the host will be provided with configuration parameters from that new policy.

There may be more than one Policy that is a match for this host/user; however, the first match found is the one that is used.

Policy assignments are not permanent. Each time a host is re-evaluated by FortiNAC, the user/host profile data is re-evaluated and a Policy is selected.

Policy overview

This section applies to all policy views.

Policy assignment

Policies are applied to hosts by comparing user and host data to the user/host profile contained in each policy until a match is found. The example below demonstrates this process.

Types

Policy Type	Location	Groups	Attributes	Time	Host Notes
Location	One or more Port or Device Groups	Any	None	Always	Host connects to a port or device in one of the selected groups and is assigned this policy.
Role	Any	Any	User Role = (Role Name)	Always	Host connects to the network. If the logged in user has the selected role, the host is assigned this policy.
Security and Access Attribute Value	Any	Any	User SaAV = (Attribute Value)	Always	Host connects to the network. If the logged in user has the selected Security and Access Value, the host is assigned this policy.
Group	Any	User Group1 User Group2	None	Always	Host connects to the network. If the logged in user is a member of either one of the selected groups, the host is assigned this policy.
Guest	Any	Any	Guest Role = Role Name	Always	Host connects to the network. If the Guest has the selected role, the host is assigned this policy.

Policy Type	Location	Groups	Attributes	Time	Host Notes
Registration	Any	Any	Host = Rogue	Always	Host connects to the network. If the host is a rogue, it is assigned this policy.
Remediation	Any	Any	Host State = At Risk	Always	Host connects to the network. If the host state is At Risk, it is assigned this policy.
VPN	Any	Any	Host = VPN Client	Always	Host connects to the network. If the host is a VPN Client, it is assigned this policy.
Time of Day	Any	Any	None	Monday - Friday 9 am to 5 pm	Host connects to the network. If the connection time is on any day Monday through Friday and between 9 am and 5 pm, it is assigned this policy.
Default or Catch All	Any	Any	None	None	This policy will match ALL hosts and users. Host connects to the network. If the host does not match any other policy, it is assigned this policy. When this policy is reached, no other policies after it will be considered.

Example endpoint compliance policy

The example below outlines how FortiNAC would choose an endpoint compliance policy for a specific host.

Assume the Host has the following characteristics:

- Connects on a port that is contained within the Library Ports group.
- Host is a member of the Accounting Group and the Finance Group.
- Host is running a Persistent Agent.
- Logged in user has a Role called Management.
- Logged in user has a Security and Access Attribute value of Accounting.

Rank	Policy	Location	Groups	Attributes	Process
1	Policy A	Port Group = Lobby Ports	Accounting	Filter1=User Role "Staff"	Location - Not a match Group - Matches Attribute1 - Not a Match Go to the next policy.

Rank	Policy	Location	Groups	Attributes	Process
2	Policy B	Port Group = Library Ports	Accounting	Filter1=User Role "Management" and User Security and Access Value "Human Resources" Filter2=User Role "Staff"	Location - Matches Group - Matches Filter1 - Does not match both pieces of data. Filter2 - Does not match. Go to the next policy.
3	Policy C	Port Group1 = Lobby Ports Port Group2 = Second Floor Ports	Finance Admin	Filter1=User Role "Staff" and User Security and Access Value "Accounting" Filter2=User Role "Management" and Host has Persistent Agent	Location - Not a match for either location. Group - Matches Finance group Filter1 - Does not match both pieces of data. Filter2 - Matches all data. In this case, the fact that neither location matches prevents the host from getting this policy. In the Group field, the host or user need only match one group. In the filter field, the host or user need only match one filter as long as it matches all parts of the filter. Go to the next policy.
4	Policy D	Any	Finance Admin	Filter1=User Role "Management" and Host has Persistent Agent Filter2=User Role "Executives" and Host has Persistent Agent	Location - No location selected so this field is not used. Group - Matches Finance group Filter1 =Matches all data Filter2 =Does not match both pieces of data This policy is selected for the host because Location is irrelevant, one group matches and one filter matches.
5	Policy E	Port Group1 = Library Ports Port Group2 = Second Floor Ports	Finance Admin	Filter1=User Role "Management" and Host has Persistent Agent Filter2=User Role "Executives" and Host has Persistent Agent	Location - Matches Port Group1 Group - Matches Finance group Filter1 =Matches all data Filter2 =Does not match both pieces of data

Rank	Policy	Location	Groups	Attributes	Process
					This policy is not selected because policies are checked in order by rank. The policy in rank 4 has already been selected even though this policy matches on more points. You must be careful about the order of the policies to ensure that the correct policy is applied to a host.

Policy details

Policy Details assesses the selected host or user and displays the specific profile and policies that apply to the host at the moment the dialog was opened. User/host profiles have a time component and hosts may be connected at different locations. Therefore, the profile and policy displayed in Policy Details now may be different than the profile and policies that display tomorrow. Each type of policy is displayed in a separate tab that also contains a Debug Log.

Note: This Debug Log can be sent to Customer Support for analysis.

To access Policy Details from Hosts:

1. Select **Users & Hosts > Hosts**.
2. Search for the appropriate host to access the context menu.
3. Select the host and right-click.
4. From the menu, select **Policy Details**.

To access Policy Details from User Accounts:

1. Select **Users & Hosts > User Accounts**.
2. Search for the appropriate user to access the context menu.
3. Select the user and right-click.
4. From the menu, select **Policy Details**.

Network Access tab settings

Field	Definition
Profile Name	Name of the user/host profile that matched the selected host or user when it was assessed by policy details. This profile contains the required criteria for a connecting host, such as connection location, host or user group membership, host or user attributes or time of day. Host connections that match the criteria within the user/host profile are assigned the associated network access policy and network access configuration. See User/host profiles on page 466 .
Policy Name	Name of the network access policy that currently applies to the host. See Network access on page 482 .

Field	Definition
Configuration Name	Name of the configuration that currently applies to the host. This is the configuration for the VLAN, CLI configuration, or VPN Group Policy for the host. See Network access configurations on page 486 .
Access Value/VLAN	The specific network access that would be provided to the host, such as a VLAN ID or Name.
CLI	Name of the CLI configuration that currently applies to this host or the connection port. This field may be blank.
Tags	Firewall Tags - defined in a Logical Network Configuration as part of a device's Model Configuration.
Debug Log	Click this link to display a log of the policy assessment process. Text within the log can be copied and pasted into a text file for analysis by Customer Support.
Edit Test	Opens the Test Policy dialog where you can simulate host, adapter, and user combinations to create test scenarios for policies and profiles. See Policy simulator on page 464 .

Authentication tab settings

Field	Definition
Profile Name	Name of the user/host profile that matched the selected host or user when it was assessed by Policy Details. This profile contains the required criteria for a connecting host, such as connection location, host or user group membership, host or user attributes or time of day. Host connections that match the criteria within the user/host profile are assigned the associated network access policy and network access configuration. See User/host profiles on page 466 .
Policy Name	Name of the authentication policy that currently applies to the host.
Configuration Name	Name of the configuration that currently applies to the host. This is the configuration for the VLAN, CLI configuration, or VPN Group Policy for the host.
Authentication Method	When enabled, the selected authentication method will override all other authentication methods configured in the portal, guest/contractor template, and Persistent Agent credential configuration.
Authentication Enabled	Indicates whether authentication is enabled. When enabled, the user is authenticated against a directory, the FortiNAC database, or a RADIUS server when logging on to access the network.
Time in Production before Authentication	When a user is waiting to authenticate, the host remains in the production VLAN until this time expires. If the user fails to authenticate within the time specified, the host is moved to the authentication VLAN.
Time Offline before Deauthentication	Once the host is offline, the user remains authenticated for this period of time. If the host comes back online before the time period ends, the user does not have to reauthenticate. If the host comes back online after the time period ends, the user is required to re-authenticate.

Field	Definition
Reauthentication Frequency	When set, this forces users to re-authenticate after the amount of time defined in this field passes since the last authentication regardless of the host's state. The host is moved to the authentication VLAN until the user reauthenticates.
Debug Log	Click this link to display a log of the policy assessment process. Text within the log can be copied and pasted into a text file for analysis by Customer Support.

Supplicant EasyConnect tab settings

Field	Definition
Profile Name	Name of the user/host profile that matched the selected host or user when it was assessed by Policy Details. This profile contains the required criteria for a connecting host, such as connection location, host or user group membership, host or user attributes or time of day. Host connections that match the criteria within the user/host profile are assigned the associated supplicant easy connect policy and supplicant configuration. See User/host profiles on page 466 .
Policy Name	Name of the most recent supplicant easy connect policy that currently applies to the host. See Supplicant EasyConnect on page 595 .
Configuration Name	Name of the configuration that currently applies to the host. This is the configuration for the supplicant on the host to allow access on a particular SSID. See Supplicant configurations on page 600 .
SSID	Name of the SSID for which the supplicant is being configured.
Security	Type of encryption used for connections to this SSID, such as WEP or WPA.
EAP Type	Currently only PEAP is supported. Not always required. This field may be blank.
Cipher	Encryption/decryption method used in conjunction with the information in the Security field to secure this connection.
Debug Log	Click this link to display a log of the policy assessment process. Text within the log can be copied and pasted into a text file for analysis by Customer Support.

Endpoint compliance tab settings

Field	Definition
Select Platform	The platform is used to determine the agent that would be assigned to the host. Not all platforms are displayed here. Only the platforms that support the Persistent Agent or Mobile Agent are displayed.
Profile Name	Name of the user/host profile that matched the selected host. This profile contains the required criteria for a connecting host, such as connection location, host or user group membership, host or user attributes or time of day. Host connections that match the criteria within the user/host profile are assigned the associated endpoint compliance policy and endpoint compliance configuration. See User/host profiles on page 466 .

Field	Definition
Policy Name	Name of the endpoint compliance policy currently applied to the selected host. See Policies on page 531 .
Configuration Name	Name of the configuration that currently applies to the host. This is the configuration for the scan and agent for the host. See Configurations on page 536 .
Scan Name	Name of the scan currently used to evaluate this host. See Scans on page 542 .
Detected Platform	The device type, such as iPhone or Android, that FortiNAC thinks the host is, based on the information currently available in the system.
Agent	Agent setting to be applied to the host. Determines whether or not an agent is used and which agent is required. Agent settings are selected in the endpoint compliance configuration.
Debug Log	Click this link to display a log of the policy assessment process. Text within the log can be copied and pasted into a text file for analysis by Customer Support.

Portal tab settings

Field	Definition
Profile Name	Name of the user/host profile that matched the selected host or user when it was assessed by Policy Details. This profile contains the required criteria for a connecting host, such as connection location. Host connections that match the criteria within the user/host profile are assigned the associated portal configuration. See User/host profiles on page 466 .
Policy Name	Name of the portal policy that currently applies to the host. See Portal policy on page 471 .
Configuration Name	Name of the portal configuration that currently applies to the host. See Content editor on page 632 .
Debug Log	Click this link to display a log of the policy assessment process. Text within the log can be copied and pasted into a text file for analysis by Customer Support.

Policy simulator

The policy simulator allows users to customize information and create scenarios to be used to virtually test policies. Instead of connecting a physical device to the network at a specific time and location in order to test a policy, the Policy Simulator allows users to test policies by virtually simulating multiple host, adapter, and user combinations. The ability to reproduce complicated scenarios without being limited to the information currently available in the system provides more accurate test results for policies, such as authentication or portal.

You can test policies from the host and user views.

Host view

1. Select **Users & Hosts > Hosts**.
2. Search for the appropriate host.
3. Select the user and right-click to access the context menu.
4. From the menu, select **Policy Details**.

5. Select the tab for the policy you want to test.
6. Click **Edit Test**.
7. In the **Test Policy** dialog, click the tabs to enter the information for each scenario you want to test.
8. Click **OK** to see the matching policy and profile to verify that the policy and profiles are correctly configured.

User view

1. Select **Users & Hosts > User Accounts**.
2. Search for the appropriate user.
3. Select the user and right-click to access the context menu.
4. From the menu, select **Policy Details**.
5. Select the tab for the policy you want to test.
6. Click **Edit Test**.
7. In the **Test Policy** dialog, click the tabs to enter the information for each scenario you want to test.
8. Click **OK** to see the matching policy and profile to verify that the policy and profiles are correctly configured.

Adapter tab

Enter information for the adapter you want to use to test the policy, or click **Populate from an Existing Adapter** to enter an existing adapter's information. See [View and search settings on page 239](#).

User tab

Enter information for the user you want to use to test the policy, or click **Populate from an Existing User** to enter an existing user's information. See [Search settings on page 199](#).

To add or change the user or administrator group, click **Group Membership**.

Host tab

Enter information for the host you want to use to test the policy, or click **Populate from an Existing Host** to enter an existing host's information. For more information, see [Settings on page 216](#).

To add or change Host Groups, click **Group Membership**.

Applications tab

Add, modify, or delete application(s) you want to use to test the policy. See [Application view on page 243](#) for information about the fields in the Applications tab.

All changes are for testing purposes only, and do not affect applications in the system.

Tests tab

Enter the required anti-spyware tests, anti-virus tests, operating system tests, and hot fix tests to test the policy. Multiple entries for each category must be comma-separated.

Date & Time tab

Select the day and time criteria to be used to test the policy.

User/host profiles

User/host profiles are used to map sets of hosts and users to Network Access policies, Endpoint Compliance policies, Authentication policies, Supplicant EasyConnect policies, Portal policies, or Security Rules (Security Incidents must be enabled). User/host profiles can be reused across many different policies.

For example, network access policies are used to assign the VLAN in which a host is placed. Each network access policy has a specific user/host profile and a network access configuration containing a VLAN, CLI configuration or VPN Group. When a host requires network access, FortiNAC looks at the network access policies starting with the first policy in the list and checks that the user/host profile is a match. If it is not, the next network access policy is checked until a match is found.

User/host profiles are combinations of user/host data. A host's or user's profile is not fixed but can change based on the user/host being moved to a different group, having a new attribute applied, connecting to the network in a different place or the current time of day. Users/hosts are only classified at the time that they need a service, such as a network access policy. When FortiNAC evaluates a host connection, the data for the user and host are prioritized as follows:

- Logged in user and host
- Registered user and host
- Registered host

If you create a user/host profile with **Where** set to **Any**, **Who/What by Group** set to **Any**, **Who/What by Attribute** set to **Any**, and **When** set to **Always**, it matches all users and hosts. This is essentially a catch all profile. If this user/host profile is used in a policy, all policies below that policy are ignored when assigning a policy to a user or a host. To highlight this, policies below the policy with the catch all profile are grayed out and have a line through the data. The best way to use a catch all profile is to create a general policy with that profile and place it last in the list of policies.

Settings

Field	Definition
Name	Each profile must have a unique name.
Who/What	Attributes A host or user must meet all parameters within a single filter, but is only required to match one filter in the list. The attribute must be known at the time of connection. See Filter example on page 468. Note: Adapter status (Adapter -> Connected -> Online/Offline) should not be used for Network Access Policies. Adapter status changes as part of the authentication process and at the time of RADIUS authentication (FNAC post-auth processing), the adapter status will always be offline. RADIUS Attributes Used to match against endpoints pre- and post-authentication. Groups

Field	Definition
	- Any — Matches any group. - Any Of — Matches any of the listed groups. Does not have to match everything, but has to match at least one group that has been selected. - All Of — Has to match every group that's been selected. - None Of — Has to match no group that's been selected.  Who/What by RADIUS Request Attribute in User/Host Profiles only works with Local RADIUS Mode. In 7.4+, Legacy Proxy will support Who/What by RADIUS Request Attribute in User/Host Profiles.
Where	Location on the network where the host is connected. This field lists groups of ports, SSIDs or devices. Hosts are checked to determine whether they have connected to the network via one of the selected devices, ports or SSIDs. Host must connect on one of the items contained within one of the selected groups to match this profile. When set to Any, this field is a match for all hosts or users. Note: For host(s) connected to FortiSwitch Port(s), please utilize Port Group and select correct port(s). Device Group with FortiSwitch selected will not result in a match.
When	If the host is on the network during the specified time frame, it matches this profile. Time options include Always or a specific set of days of the week and times of the day.
Notes	User specified note field. This field may contain notes regarding the data conversion from a previous version of FortiNAC.
Last Modified By	User name of the last user to modify the profile.
Last Modified Date	Date and time of the last modification to this profile.
Right click options	
Edit	Opens the Create view pre-populated with the settings from the selected Profile.
Copy	Copy the selected Profile to create a new record.
Delete	Deletes the selected Profile. Profiles that are currently in use cannot be deleted.
Used By	Indicates whether or not the selected Profile is currently being used by any other FortiNAC element. See Profiles in use on page 470 .
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746 .

Field	Definition
	 You must have permission to view the admin auditing log. See Add an administrator profile on page 139.

Add or modify a profile

You are not required to complete all of the fields when creating a user/host profile. If you leave a field blank, it is set to Any or is left blank. When set to Any or blank, the field is a match for all hosts or users. You can create a profile with only location, only a group, only an attribute filter, only a time range or any combination of those options.

1. Select **Policy & Objects**.
2. Select **User/Host Profiles**.
3. Click **Create New** or select an existing Profile and click **Edit**.
4. Click in the **Name** field and enter a name for this Profile.
5. Specify the details according to the User/Host profiles settings listed above.



If the user wishes to configure multiple attributes in a single line in an AND relationship, the user should use the + at the far right. However, if the user wishes to configure the attributes in an OR relationship, the user should use the + at the bottom.

6. Click **OK** to save your data.

Attributes

A host or user must meet all parameters within a single filter, but is only required to match one filter in the list. The attribute must be known at the time of connection. See [Filter example on page 468](#).

Note: Adapter status (Adapter -> Connected -> Online/Offline) should not be used for Network Access Policies. Adapter status changes as part of the authentication process and at the time of RADIUS authentication (FNAC post-auth processing), the adapter status will always be offline.

RADIUS Attributes

Used to match against endpoints pre- and post-authentication.

Groups

- Any — Matches any group.
- Any Of — Matches any of the listed groups. Does not have to match everything, but has to match at least one group that has been selected.
- All Of — Has to match every group that's been selected.
- None Of — Has to match no group that's been selected.

Filter example

User/host profiles contain filters to narrow the group of hosts or users that match a particular profile. This allows you to create special profiles for certain hosts or users and filter by host, adapter, user criteria, or RADIUS attribute. For example, if you had hosts that were running on different operating systems, you might want to have a special profile for

each operating system. By filtering for the operating system, you could provide different treatment for each type of host without having to create and maintain special host groups.

Filter examples

Filters are based on Host, Adapter, User, Application, and RADIUS attributes and can be applied such that the host or user must meet all criteria or only some criteria. Within the Who/What by Attribute filter, the user/host must match all of the data specified. If there are multiple Who/What by Attribute filters, the user/host must match all of the data specified in only one of the filters.

Assume that you want to create user/host profile A to handle rogue hosts by operating system. In this case, the host must meet the following criteria to match user/host profile A:

- **Location** = Connected to a device in Device Group A
- **Host Filter** = Running a Windows operating system and is a Rogue (not registered).

In the second example, the user/host profile contains two options under Who/What by Attribute. The first filter requires that the host state be Safe and Authenticated. The second filter requires that the host be a VPN client. In this case the host must meet the following criteria to match the user/host profile:

- **Location** = Connected to a device in Device Group A
- **Host Filter** = One of the following sets of options from the filters:
 - Host must be Safe and Authenticated
 - Host must be a VPN Client

Profile example

Assume that you are running a network at a University. You have Students and Faculty that must be allowed on the network. Due to the volume of traffic, you determine that you will have four VLANs. This division of network users requires a mechanism for matching them to the appropriate VLANs. To accomplish this task, you must do the following:

- Determine how you are going to divide your network users into four groups. In this case you decide that you will break up users as follows:
 - Students that connect to devices in Dorm A
 - Students that connect to devices in Dorm B
 - Faculty running Windows
 - Faculty running macOS
- Make sure that Students are in a group labeled Students and Faculty are in a group labeled Faculty.
- Make sure that you have two device groups, one for devices in Dorm A and another for devices in Dorm B.
- Based on the divisions you have selected, you must create four user/host profiles. You need one profile for each combination of data that defines a set of users, such as Students that connect to devices in Dorm A.
- Create four network access configurations to configure the VLANs for your four groups of users.
- Create four network access policies to map the four user/host profiles to the appropriate VLANs.

User/host profiles

Create four user/host profiles that have the following settings:

Name	Where	Who/What by Group	Who/What by Attribute	Time
Students Dorm A	Device Group = Dorm A Devices	User Group = Students	None	Always
Students Dorm B	Device Group = Dorm B Devices	User Group = Students	None	Always
Faculty Windows	Any	User Group = Faculty	Host OS = Windows	Always
Faculty macOS	Any	User Group = Faculty	Host OS = macOS	Always

Network access configurations

Create a network access configuration for each of the four VLANs that you wish to assign. For this example we will create configurations for VLANS 10, 20, 30 and 40.

Name	Access Value
Students Dorm A VLAN	10
Students Dorm B VLAN	20
Faculty Windows VLAN	30
Faculty macOS VLAN	40

Network access policies

Now you must map the user/host profiles to the network access configurations you created. That will tie the different types of users to the appropriate VLAN. Create four network access policies that contain the following data:

Name	User/host profile	Network access configuration
Students Connecting in Dorm A	Students Dorm A	Students Dorm A VLAN
Students Connecting in Dorm B	Students Dorm B	Students Dorm B VLAN
Faculty running Windows	Faculty Windows	Faculty Windows VLAN
Faculty running macOS	Faculty macOS	Faculty macOS VLAN

Profiles in use

To find the list of FortiNAC features that reference a specific user/host profile, select the profile from the **User/Host Profiles View** and click **Used By**. A panel is displayed indicating whether or not the profile is associated with any other features. If the profile is referenced elsewhere, a list of each feature that references the profile is displayed.

Delete a profile

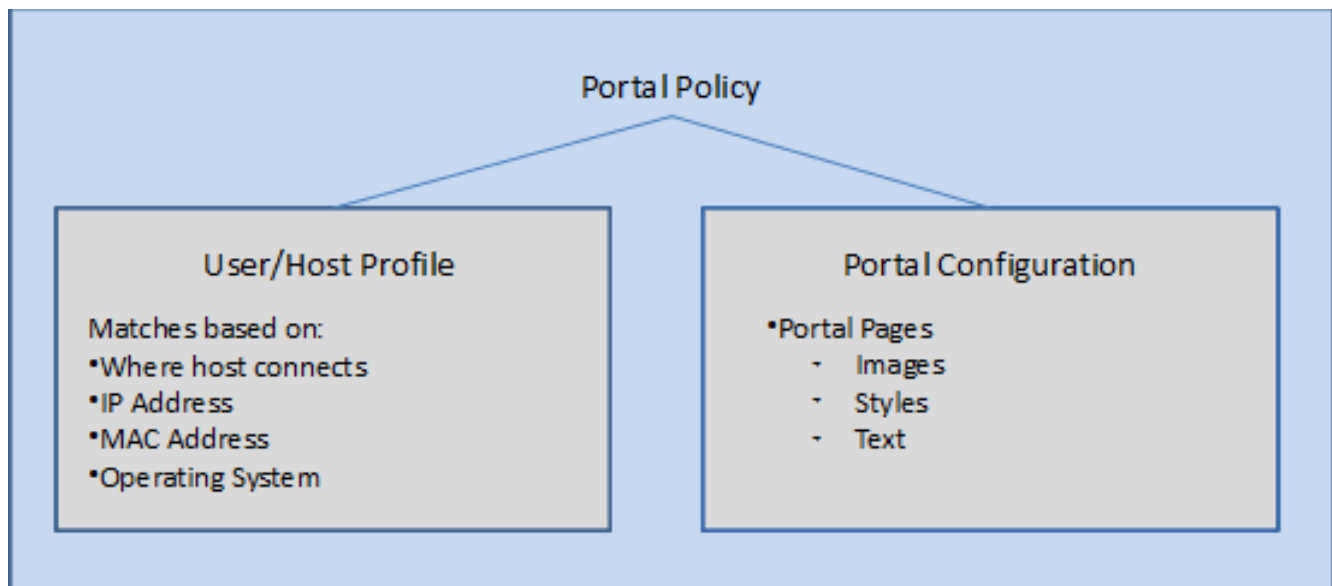
1. Click **Policy & Objects**.
2. Select **User/Host Profiles**.
3. Select the profile to be removed.
4. Click **Delete**.
5. Click **OK** to confirm that you wish to remove the profile.



When attempting to delete a profile which is currently being used by other elements, an error message will be displayed stating "One or more selected User/Host Profiles are currently in use" - it will not list which items are using it. The user would need to then access the "Used By" action to see which items are using it.

Portal policy

A Portal Policy consists of one user/host profile and one portal configuration. The user/host profile is used to determine the hosts to which this policy might apply. The portal configuration controls the look and feel of the portal pages displayed to those users and hosts when they connect to the network and register. Portal Policies determine the portal assigned to a connecting host in an environment where there are multiple portals.



Portal Policies rely on a limited set of host information to match a portal configuration with a user/host profile. When an unregistered host connects to the network, there are only a few pieces of data that are known about the host and no data is known about the user. Therefore, the user/host profile used in a Portal Policy can only use the connection location, the host IP address, the host MAC address or the operating system to match a connecting host.

Portal Policies are ranked with 1 being the highest rank. When a host connects to the network, the policies are evaluated from the highest rank down until a matching policy is found. That policy is assigned to the host and the portal when the policy is displayed.



There may be more than one Portal Policy that is a match for this host/user; however, the first match found is the one that is used.

If you create a user/host profile with fields Where set to Any, Who/What by Group set to Any, Who/What by Attribute set to Any and When set to Always, it matches ALL users and hosts. This is essentially a Catch All profile. If this user/host profile is used in a policy, all policies below that policy are ignored when assigning a policy to a user or a host. To highlight this, policies below the policy with the catch all profile are grayed out and have a line through the data.

The best way to use a Catch All profile is to create a general policy with that profile and place it last in the list of policies.

If a host does not match any of the policies listed, FortiNAC connects the host to the user-specified default portal. See [Select a default portal on page 733](#).

Implementation

- Create a separate portal configuration for each group of users that requires different treatment. See [Multiple portals on page 633](#).
- Create a user/host profile for each type of user, but base the profile on Host attributes that can be discovered when the host connects to the network, such as connection location, IP address, MAC address, or operating system. See [User/host profiles on page 466](#).
- Create a Portal Policy for each group of users that requires different treatment. See [Manage policies on page 472](#).

Manage policies

Create Portal Policies to assign a portal when an unregistered host connects to the network. Policies are selected for a connecting host by matching host attributes to the criteria defined in the associated user/host profile. The first policy that matches the host data is assigned.



If the host does not match any policy, it is assigned the default Portal. See [Select a default portal on page 733](#).

Settings

An empty field in a column indicates that the option has not been set.

Field	Definition
Rank	Policy's rank in the list of policies. Rank controls the order in which host connections are compared to Policies.
Enabled	Indicates if the policy is enabled/disabled.
Name	User defined name for the policy.
Configuration	Contains the configuration for the portal that will be assigned if this Portal Policy matches the connecting host. See Content editor on page 632 .

Field	Definition
Who/What	Attributes A host or user must meet all parameters within a single filter, but is only required to match one filter in the list. The attribute must be known at the time of connection. See Filter example on page 468. Note: Adapter status (Adapter -> Connected -> Online/Offline) should not be used for Network Access Policies. Adapter status changes as part of the authentication process and at the time of RADIUS authentication (FNAC post-auth processing), the adapter status will always be offline. RADIUS Attributes Used to match against endpoints pre- and post-authentication. Groups - Any — Matches any group. - Any Of — Matches any of the listed groups. Does not have to match everything, but has to match at least one group that has been selected. - All Of — Has to match every group that's been selected. - None Of — Has to match no group that's been selected.
Where	The connection location specified in the user/host profile. The host must connect to the network on a device, port or SSID contained within one of the groups shown here to be a match. When set to Any, this field is a match for all hosts or users.
When	The time frame specified in the selected user/host profile. The host must be on the network within this time frame to be a match. When set to Always, this field is a match for all hosts or users.
Notes	User specified note field. This field may contain notes regarding the data conversion from a previous version of FortiNAC.
Right click options	
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746.  You must have permission to view the admin auditing log. See Add an administrator profile on page 139.

Create or edit a policy

1. Select **Policy & Objects**.
2. Select **Portal Policy**.
3. Click **Create New** or select an existing policy and click **Edit**.
4. Fill out the fields in accordance with the following settings:

Field	Definition
Name	Each profile must have a unique name.
Notes	User specified note field. This field may contain notes regarding the data conversion from a previous version of FortiNAC.
Configuration	Select a portal configuration from the drop-down menu. If the portal configuration you need is not shown, you must go to the portal content editor and create it before adding the Portal Policy. See Multiple portals on page 633 .
User/Host profile	Select a user/host profile from the drop-down menu. If the user/host profile you need is not shown, you can create a new one by leaving the drop-down selection at "Create New" and populating the Conditions fields as desired. Likewise, a user/host profile can be copied from an existing entry by selecting it in the drop-down and changing the toggle in the Conditions section from "Use Existing" to "Clone", and then making desired edits to the fields. An existing user/host profile can also be edited from this view by clicking the pencil icon next to the entry in the drop-down. See User/host profiles. Creating a new UHP  The user can also create a new UHP in this view by leaving the default selection at "Create New" and populating the Conditions fields below. Likewise, a UHP can be copied from an existing UHP by selecting it in the list and changing the toggle from "Use Existing" to "Clone" and making edits to the Conditions fields as desired. An existing UHP can also be edited from this view by clicking the pencil icon in the drop down next to the item to be edited.
Conditions	
Use Existing	Directly uses the selected user/host Profile (not editable) as is.
Clone	Copies the user/host Profile config into its own profile, allowing the user to edit the settings. A name would need to be specified in order to uniquely identify the cloned UHP.
Who/What	Attributes A host or user must meet all parameters within a single filter, but is only required to match one filter in the list. The attribute must be known at the time of connection. See Filter example on page 468. Note: Adapter status (Adapter -> Connected -> Online/Offline) should not be used for Network Access Policies. Adapter status changes as part of the authentication process and at the time of RADIUS authentication (FNAC post-auth processing), the adapter status will always be offline. RADIUS Attributes Used to match against endpoints pre- and post-authentication. Groups Any — Matches any group.

Field	Definition
	- Any Of — Matches any of the listed groups. Does not have to match everything, but has to match at least one group that has been selected. - All Of — Has to match every group that's been selected. - None Of — Has to match no group that's been selected.
Where	Location on the network where the host is connected. This field lists groups of ports, SSIDs or devices. Hosts are checked to determine whether they have connected to the network via one of the selected devices, ports or SSIDs. Host must connect on one of the items contained within one of the selected groups to match this profile. When set to Any, this field is a match for all hosts or users.
When	If the host is on the network during the specified time frame, it matches this profile. Time options include Always or a specific set of days of the week and times of the day.
Right click options	
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746 .
	 You must have permission to view the admin auditing log. See Add an administrator profile on page 139.
Buttons	
Disable	Shuts off the Policy. Whatever is defined in the policy that is disabled is not in effect.

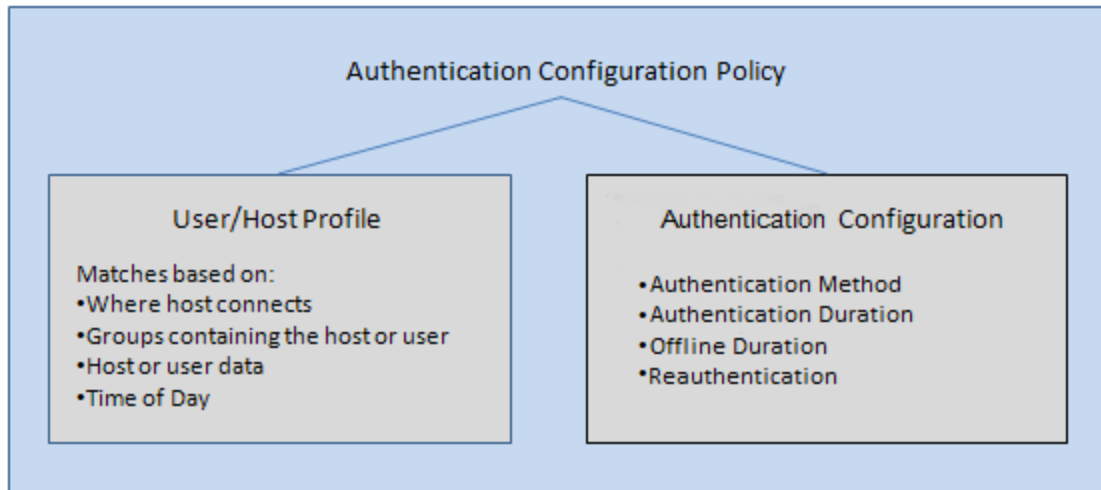
5. Click **OK** to save your Policy.

Delete a policy

1. Select **Policy & Objects**.
2. Select **Portal**.
3. Select a Policy and click **Delete**.
4. A confirmation message is displayed. Click **Yes** to continue.

Authentication

An authentication policy consists of one user/host profile and one authentication configuration. The user/host profile is used to determine the users and hosts to which this policy might apply. The authentication configuration assigns the treatment those users and hosts receive when they connect to the network.



The authentication configuration specifies the time in production before authentication, time offline before deauthentication, reauthentication frequency, and authentication method policy that apply to a host that requires network access.

When authentication method is enabled, the selected authentication is used instead of the default authentication method. This authentication method will override the authentication methods selected for the portal login, guest/contractor template, and the Persistent Agent credential configuration. For example, if the portal configuration for the user's portal had a standard user login type of LDAP, but the user matched an authentication policy with the authentication configuration set to local, local will be used instead. If the authentication method is not enabled, the default authentication method is used.

Policies are assigned based on matching data when a host requires network access. The host/user and the connection location are compared to each authentication policy starting with the first policy in the list. When a policy is found where the host and user data and the connection location match the selected user/host profile, that policy is assigned. Policy assignments are not permanent. Hosts are re-evaluated frequently, such as when a switch is polled or the Persistent Agent contacts the server. When host and user data are re-evaluated a different authentication policy may be selected.



There may be more than one authentication policy that is a match for this host/user; however, the first match found is the one that is used.

If you create a user/host profile with fields Where set to Any, Who/What by Group set to Any, Who/What by Attribute set to Any and When set to Always, it matches ALL users and hosts. This is essentially a Catch All profile. If this user/host profile is used in a policy, all policies below that policy are ignored when assigning a policy to a user or a host. To highlight this, policies below the policy with the catch all profile are grayed out and have a line through the data.

The best way to use a Catch All profile is to create a general policy with that profile and place it last in the list of policies.

Manage policies

Create authentication policies to assign an authentication configuration when a host requires network access. Policies are selected for a connecting host by matching host and user data to the criteria defined in the associated user/host profile. The first policy that matches the host and user data is assigned.



If the host does not match any policy, it is assigned the default authentication method configured in the Portal, guest template, or Persistent Agent Credential Configuration.

If you create a user/host profile with fields Where set to Any, Who/What by Group set to Any, Who/What by Attribute set to Any and When set to Always, it matches ALL users and hosts. This is essentially a Catch All profile. If this user/host profile is used in a policy, all policies below that policy are ignored when assigning a policy to a user or a host. To highlight this, policies below the policy with the catch all profile are grayed out and have a line through the data.

The best way to use a Catch All profile is to create a general policy with that profile and place it last in the list of policies.

Authentication policies can be accessed from **Policy & Objects > Authentication Policy**.

Settings

An empty field in a column indicates that the option has not been set.

Field	Definition
Rank	Policy's rank in the list of policies. Rank controls the order in which host connections are compared to Policies.  Set Rank is now legacy architecture. In 7.2, use drag and drop to reorder the rank from the left column, click edit from within the cell.
Configuration	Contains the configuration for the authentication policy that will be assigned if this authentication policy matches the connecting host. See Authentication configurations on page 479
Who/What	Attributes User or Host attributes specified in the selected user/host profile. The connecting host or user must have the attributes to be a match. See Filter example on page 468. Do not select user attributes in user/host profiles used to assign a portal. FortiNAC does not have access to any user attributes when an unregistered host connects to the network. Only the following host attributes are known at the time of connection: connection location, IP address, MAC address, and operating system. RADIUS Attributes Indicates whether or not attribute filters have been created for this Profile. RADIUS attribute filters are used to match against endpoints pre- and post-authentication. Groups User or Host group or groups specified in the user/host profile. These groups must contain the connecting user or host for the connection to be a match for this policy. When set to Any, this field is a match for all hosts or users. It is not recommended that you use groups in user/host profiles for Portal assignment because an unregistered host will not be contained in any host groups and user data is unknown until after the portal is assigned.

Field	Definition
Where	The connection location specified in the user/host profile. The host must connect to the network on a device, port or SSID contained within one of the groups shown here to be a match. When set to Any, this field is a match for all hosts or users.
When	The time frame specified in the selected user/host profile. The host must be on the network within this time frame to be a match. When set to Always this field is a match for all hosts or users.
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746 .
 You must have permission to view the admin auditing log. See Add an administrator profile on page 139 .	

Create or edit a policy

1. Select **Policy & Objects**.
2. Select **Authentication Policy**.
3. Click **Create New** or select an existing policy and click **Edit**.
4. Click in the **Name** field and enter a name for this policy.
5. Enable or disable the policy.
6. Select a **User/Host Profile** from the drop-down menu. Note: If you modify this profile, it is modified for all features that make use of the profile. Connecting hosts must match this user/host profile to be assigned the authentication configuration specified in the next step.
7. Select an authentication configuration from the drop-down menu. Note that if you modify this configuration, it is modified for all features that make use of it. See [Create or edit a configuration on page 487](#).
8. Click **OK** to save your policy.

Delete a policy

If a configuration is in use by another feature in FortiNAC, it cannot be deleted. A dialog displays with a list of the features in which the configuration is used. Remove the association between the configuration and other features before deleting the configuration.

1. Click **Policy & Objects**.
2. Select **Authentication Policy**.
3. Select the policy to be removed.
4. Click **Delete**.
5. Click **OK** to confirm that you wish to remove the policy.

When no profile or policy exists

The following describes authentication scenarios when no authentication profile or policy exists. In these cases, authentication was done via LDAP using the configuration in **System > Settings > Authentication > LDAP**.

Without an authentication policy, no host is marked with a red "A" to indicate the need to authenticate or to force authentication.

Wired connection and wireless MAC auth (authentication set to enforce)

You must have a Passive Agent configuration set up in order to obtain logged on users via the Passive Agent.

When the Passive Agent configuration is set to Register Host by User and a directory user logs into the host/domain where the rogue is registered, a logged on user is displayed. The logged on user is the user who is logged onto the domain. When the user logs off the domain, the logged on user in FortiNAC is removed.

If the Passive Agent configuration is not set to register the host, the host must register by another method. Once registered whenever the host is logged onto a domain, the logged on user will be set to the domain user.

If an online host with a logged on user disconnects before logging off the user, the logged on user is removed from the host after 10 minutes. A red "A" is displayed with the offline host, indicating a need to authenticate. If the host connects with or without user information from the Passive Agent, the red "A" is no longer displayed.

802.1X with the Passive Agent (authentication set to enforce)

This scenario is similar to the wired connection and wired MAC auth (authentication set to enforce) scenario, except the logged on user is initially set to the 802.1x user, and is then switched to the user logged onto the domain.

802.1X without Passive Agent (authentication set to enforce)

When registered via the Portal, the logged on user is displayed as the 802.1x user.

Wired connection registering via the pop up dialog provide by the PA

The rogue is connected to a port that is not in forced authentication. After entering directory credentials the host is registered to that user, and there is no logged on user.

Authentication configurations

Authentication configurations define authentication methods for connecting hosts and users. Users can enable hosts to authenticate using a specific authentication method, define authentication duration, and require reauthentication after a defined time period. The authentication configuration that is assigned to a particular host is determined by the pairing of an authentication configuration and a user/host profile within an authentication policy.

Enabling authentication allows the Administrator to determine whether or not hosts connecting to the network will be forced to authenticate. Hosts can be forced to reauthenticate after a specified period of time.

Settings

Field	Definition
Add Filter	Allows you to select a field from the current view to filter information. Select the field from the drop-down list, and then enter the information you wish to filter.
Update Button	Displays the filtered data in the table.
Table columns	
Name	The name of the authentication configuration.
Time in Production before Authentication	When a user is waiting to authenticate, the host remains in the production VLAN until this time expires. If the user fails to authenticate within the time specified, the host is moved to the authentication VLAN.
Time Offline before Deauthentication	Once the host is offline, the user will remain authenticated for this period of time. If the host comes back online before the time period ends, the user will not need to re-authenticate. If the host comes back online after the time period ends, the user will be required to re-authenticate. Hosts which don't match a User/Host profile that is associated with an authentication policy Configuration will be deauthenticated after the system default time of 10 minutes. To ensure that all hosts get an authentication policy, create a "Catch All" User/Host profile and associate it to an authentication configuration.
Reauthentication Frequency	When set, this forces users to re-authenticate after the amount of time defined in this field passes since the last authentication regardless of the host's state. The host is moved to the authentication VLAN.
Authentication Method	When enabled, the selected authentication method will override all other authentication methods configured in the portal, guest/contractor template, and Persistent Agent Credential configuration.
Invalid Credentials Method	Enables you to modify the error message displayed in the Portal and Persistent Agent when a user fails to successfully authenticate.
Note	User-defined information about the policy configuration.
Last Modified By	User name of the last user to modify the policy configuration.
Last Modified Date	Date and time of the last modification to this policy.
Right click options	
Delete	Deletes the selected authentication configuration.
Modify	Opens the modify authentication configuration window for the selected configuration. See Add or modify a policy on page 481
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746 .
 You must have permission to view the admin auditing log. See Add an administrator profile on page 139.	

Add or modify a policy

1. Select **Policy & Objects**.
2. Select **Authentication**.
3. Click **Add** or select an existing policy and click **Modify**.
4. Enter a name for the policy.
5. Use the settings below to configure the new authentication policy.
6. Click **OK** to save your policy.

Settings

Field	Definition
Name	Enter a name that describes the policy configuration.
Authentication Method	When enabled, the selected authentication method will override all other authentication methods configured in the portal, guest/contractor template, and Persistent Agent credential configuration.
Invalid Credentials Message	Enables you to modify the error message displayed in the portal and Persistent Agent when a user fails to successfully authenticate.
Enable Authentication	When enabled, the user is authenticated against a directory, the FortiNAC database, or a RADIUS server when logging on to access the network.
Time in Production before Authentication	When a user is waiting to authenticate, the host remains in the production VLAN until this time expires. If the user fails to authenticate within the time specified, the host is moved to the authentication VLAN.
Time Offline before Deauthentication	Once the host is offline, the user will remain authenticated for this period of time. If the host comes back online before the time period ends, the user will not need to re-authenticate. If the host comes back online after the time period ends, the user will be required to re-authenticate. Hosts which don't match a user/host profile that is associated with an authentication policy configuration will be deauthenticated after the system default time of 10 minutes. To ensure that all hosts get an authentication policy, create a catch all user/host profile and associate it to an authentication configuration.
Reauthentication Frequency	When set, this forces users to re-authenticate after the amount of time defined in this field passes since the last authentication regardless of the host's state. The host is moved to the authentication VLAN.
Note	Allows users to enter additional information about the policy.

Delete a configuration

1. Click **Policy & Objects**.
2. Select **Authentication Policy**.
3. Select **Configuration** from the menu.

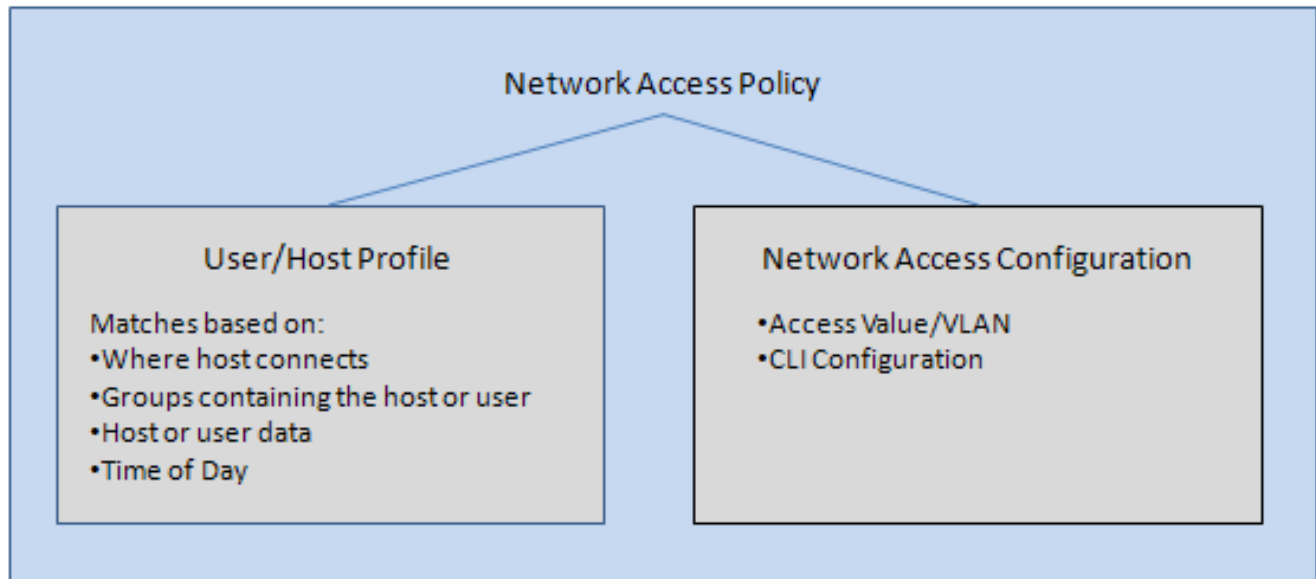
4. Select the authentication configuration to be removed.
5. Click **Delete**.
6. Click **OK** to confirm that you wish to remove the configuration.

Network access

A network access policy consists of one user/host profile and one network access configuration. The user/host profile is used to determine the users and hosts to which this policy might apply. The network access configuration assigns the treatment those users and hosts receive when they connect to the network.



Network access policies are used for registered hosts only.



The network access configuration specifies the VLAN, CLI configuration or VPN Group Policy that apply to a host that requires network access. If the user or host matches the selected user/host profile they are given the network access defined in the configuration.

Network access policies follow a pattern, such as when anyone in group X of people connects to a device in group Y of devices only put those users on VLAN 10. Devices that are end-stations, such as a gaming device, a printer or a medical device can be treated as if they were people. For example, if a gaming device that matches the specified user/host profile is connected to a switch that also matches the user/host profile it can be moved to a special VLAN for gaming devices defined in the network access configuration.

Network access policies are very flexible and can be used in more complex situations. For example, network access policies can be created for medical devices that are end stations. When a medical device is connected to any port in the hospital, FortiNAC can use a network access policy that contains a CLI configuration to reduce the rate of data transfer on those ports.

Network access policies can also be used to pass a group policy to a user connecting through a VPN concentrator. When a user connects through a VPN you do not want to disconnect the user in order to move the user from one VLAN to another. However, when the user is authenticated and the authentication is returned to the VPN concentrator, FortiNAC can also send a group policy for that user. The policy can then restrict the user's network access to certain areas. Group policies are configured on the VPN concentrator. When the name of the Group policy is entered into the Access Value/VLAN field on the **Network Access Configuration** window, that VPN group policy is then enforced for the connecting user.

Policies are assigned based on matching data when a host requires network access. The host/user and the connection location are compared to each network access policy starting with the first policy in the list. When a policy is found where the host and user data and the connection location match the selected user/host profile, that policy is assigned. Policy assignments are not permanent. Hosts are re-evaluated frequently, such as when a switch is polled or the Persistent Agent contacts the server. When host and user data are re-evaluated a different network access policy may be selected.



There may be more than one network access policy that is a match for this host/user; however, the first match found is the one that is used.

If you create a user/host profile with fields Where set to Any, Who/What by Group set to Any, Who/What by Attribute set to Any and When set to Always, it matches ALL users and hosts. This is essentially a Catch All profile. If this user/host profile is used in a policy, all policies below that policy are ignored when assigning a policy to a user or a host. To highlight this, policies below the policy with the catch all profile are grayed out and have a line through the data.

The best way to use a Catch All profile is to create a general policy with that profile and place it last in the list of policies.

Implementation

- Determine which device(s) will be used to support a specific network access policy.
- Configure the device(s) with the VLAN or Interface ID information for the network access policy. **Note:** Network Access Policy application to switches without the specified VLAN configured may cause unexpected results.
- Create a device group and add the device(s) for each set of devices that will be used for network access policies. For example, you might have a group of devices that provide network access in Building A. That group of devices will provide different types of access than the devices in Building B, therefore you would create two separate device groups. See [Groups on page 843](#) for information on groups.
- If only some ports on a device or devices will be used for network access policies, you can place just the required ports in a Port group specifically for use in network access policies. First, determine which ports will participate in network access policies and place those ports in the Role Based Access Group. Ports that are not in this group cannot apply policies. Once ports are in the Role Based Access group, place them in groups that will be associated with specific user/host profiles and network access policies. See [Groups on page 843](#) for information on groups. Ports that are designated as connection locations for network access policies are typically included in the Role Based Access Group. If a port is used in a policy but is not included in the Role Based Access Group, devices connecting to that port are placed in the default VLAN entered on model configuration for that device. They are not placed on the VLAN defined for the network access policy.
- Determine which hosts or users will receive which network access. Create user/host profiles that would match each set of Users or Hosts that require different treatment. For example, if you want your Executives on VLAN 10 and you Admin Staff on VLAN 20 you must create a user/host profile for each set of users. See [User/host profiles on page 466](#).
- Create a network access configuration for each VLAN, CLI configuration or VPN Group Policy that you wish to assign to connecting hosts. See [Network access configurations on page 486](#).

- Create your network access policies by mapping a user/host profile to a network access configuration. See [Network access on page 482](#).

Manage policies

Create network access policies to assign a VLAN, implement a CLI configuration or assign a VPN Group Policy when a host requires network access. Policies are selected for a connecting host by matching host and user data to the criteria defined in the associated user/host profile. The first policy that matches the host and user data is assigned.



If the host does not match any policy, it is assigned the default VLAN configured on the switch.

If you create a user/host profile with fields Where set to Any, Who/What by Group set to Any, Who/What by Attribute set to Any and When set to Always, it matches ALL users and hosts. This is essentially a Catch All profile. If this user/host profile is used in a policy, all policies below that policy are ignored when assigning a policy to a user or a host. To highlight this, policies below the policy with the catch all profile are grayed out and have a line through the data.

The best way to use a Catch All profile is to create a general policy with that profile and place it last in the list of policies.

Settings

An empty field in a column indicates that the option has not been set.

Field	Definition
Rank	Policy's rank in the list of policies. Rank controls the order in which host connections are compared to Policies.  Set Rank is now legacy architecture. In 7.2, use drag and drop to reorder the rank from the left column, click edit from within the cell.
Name	User defined name for the policy.
Configuration	Contains the configuration for the VLAN, CLI configuration or VPN Group Policy that will be assigned if this Access Policy matches the connecting host. See Network access configurations on page 486 .
Who/What	Attributes A host or user must meet all parameters within a single filter, but is only required to match one filter in the list. The attribute must be known at the time of connection. See Filter example on page 468. Note: Adapter status (Adapter -> Connected -> Online/Offline) should not be used for Network Access Policies. Adapter status changes as part of the authentication process and at the time of RADIUS authentication (FNAC post-auth processing), the adapter status will always be offline. RADIUS Attributes Used to match against endpoints pre- and post-authentication.

Field	Definition
	Groups - Any — Matches any group. - Any Of — Matches any of the listed groups. Does not have to match everything, but has to match at least one group that has been selected. - All Of — Has to match every group that's been selected. - None Of — Has to match no group that's been selected.
Where	The connection location specified in the user/host profile. The host must connect to the network on a device, port or SSID contained within one of the groups shown here to be a match. When set to Any, this field is a match for all hosts or users.
When	The time frame specified in the selected user/host profile. The host must be on the network within this time frame to be a match. When set to Always this field is a match for all hosts or users.
Used By	Lists all elements which are using this component.
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746.  You must have permission to view the admin auditing log. See Add an administrator profile on page 139.

Create or edit a policy

1. Select **Policy & Objects**.
2. Select **Network Access**.
3. Click **Create New** or select an existing Policy and click **Edit**.
4. Click in the **Name** field and enter a name for this Policy.
5. Select a **User/Host Profile** from the drop-down menu. Note that if you modify this profile, it is modified for all features that make use of the profile. Connecting hosts must match this user/host profile to be assigned the network access configuration specified in the next step.
6. Select a configuration from the drop-down menu. Note that if you modify this configuration, it is modified for all features that make use of it. See [Create or edit a configuration on page 487](#).
7. The **Note** field is optional.
8. Click **OK** to save your policy.

Delete a policy

1. Click **Policy & Objects**.
2. Select **Network Access**.
3. Select the policy to be removed.

4. Click **Delete**.
5. Click **OK** to confirm that you wish to remove the policy.

Network access configurations

Network access configurations define access treatments for connecting hosts and users. Hosts can be placed in a particular VLAN, have a CLI configuration applied or be passed a VPN Group Policy. The network access configuration that is assigned to a particular host is determined by the pairing of a network access configuration and a user/host profile within a network access policy.

When a host requires network access, the host and user are compared to the user/host profile in each network access policy starting with the first policy in the list. When a policy is found where the host and user data match the user/host profile in the policy, that policy is assigned. The network access configuration contained within that policy specifies the treatment received by the host.

Settings

An empty field in a column indicates that the option has not been set.

Field	Definition
Name	User defined name for the Configuration.
Logical Network	The Logical Network to assign. Logical networks are access values that translate to the physical value of network infrastructure devices. They are used to separate network access policies from device specific values. See Logical networks .
Note	User specified note field. This field may contain notes regarding the conversion from a previous version of FortiNAC.
Last Modified By	User name of the last user to modify the configuration.
Last Modified Date	Date and time of the last modification to this configuration.
Right click options	
Delete	Deletes the selected network access configuration.
In Use	Indicates whether or not the selected configuration is currently being used by any other FortiNAC element. See Configurations in use on page 487 .
Modify	Opens the Modify Network Access Configuration window for the selected configuration.
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746 .
 You must have permission to view the admin auditing log. See Add an administrator profile on page 139.	

Create or edit a configuration

1. Select **Policy & Objects**.
2. Expand **Network Access**.
3. Select **Configuration**.
4. On the **Network Access Configurations** window, click **Create New** or select an existing configuration and click **Edit**.
5. Click in the **Name** field and enter a name for this configuration.
6. If you are using an alias instead of an actual Access Value, enable the **Access Value is an alias** check box. This indicates that the Access Value/VLAN field contains an Alias that represents many VLANs across multiple devices on your network.
7. Select a **Logical Network** from the drop down to assign to the configuration.
8. The **Note** field is optional.
9. Click **OK** to save the configuration.

Configurations in use

To find the list of FortiNAC features that reference a specific network access configuration, select the configuration from the **Network Access Configurations** view and click **In Use**. A message is displayed indicating whether or not the configuration is associated with any other features. If the configuration is referenced elsewhere, a list of each feature that references the configuration is displayed.

Delete a configuration

If a configuration is in use by another feature in FortiNAC, it cannot be deleted. A dialog displays with a list of the features in which the configuration is used. Remove the association between the configuration and other features before deleting the configuration.

1. Click **Policy & Objects**.
2. Expand **Network Access**.
3. Select **Configuration** from the menu.
4. Select the configuration to be removed.
5. Click **Delete**.
6. Click **OK** to confirm that you wish to remove the configuration.

Endpoint compliance

Endpoint compliance is a feature set used to ensure that hosts connecting to your network comply with network usage requirements. The cornerstone of endpoint compliance are endpoint compliance policies. Use these policies to establish the parameters for security that will be enforced when hosts connect to the network. If you do not create policies, when hosts connect to the network and users enter their credentials, they will be automatically registered without a policy being applied. See [Policies on page 531](#).

Endpoint compliance can also use an agent on the host to ensure that compliance with established policies is maintained. The Dissolvable Agent is downloaded during registration and is removed when the host is registered. The Persistent Agent remains on the host. Mobile Agent devices are installed on and remain installed on mobile devices. The Passive Agent is not installed, but is served as the user logs onto the network and does a scan in the background.

Endpoint compliance policies contain scans used to evaluate hosts and ensure that each host complies with your configured list of acceptable operating systems and antivirus software. For a list of supported operating systems and antivirus software, use the customer portal on our web site.

Features

Feature	Description
Agent Distribution	Download Agents for alternative distribution. See Agent packages on page 992 .
Auto-Def Update Schedule	Schedule the task to automatically update virus definitions, spyware definitions and operating systems for which you can scan. See Auto-definition updates on page 531 .
NAT Detection	Enter the IP ranges where an agent will detect NAT'd hosts. IP addresses outside this range could be NAT'd hosts and can generate an event and an alarm to notify the network administrator. See NAT detection on page 888 .
Passive Agent Configuration	Create customized configurations that register and scan hosts associated with network users contained in your LDAP or Active directory. See Passive Agent on page 604 .
Policy Configuration	Add, delete, modify, or schedule endpoint compliance policy. See Policies on page 531 .
Persistent Agent Properties	Enter text that will be displayed in the header and footer area on any messages sent to a host running the Persistent Agent. Enable status pop-ups. Configure server communication. See Persistent Agent on page 913 .
Remediation Configuration	Add, remove, modify, or schedule security and admin script profile configurations. See Remediation configurations on page 615 .

Implementation

Endpoint compliance allows you to create security policies and use those policies to scan network users' computers for compliance with your organization's network usage rules. The implementation of this feature set can vary widely from one organization to another based on how restrictive or open you choose to make it. You can simply monitor hosts for non-compliance or go so far as to completely block network access. You can institute scans based on simple options included in FortiNAC or create your own custom scans. This section of the documentation discusses the implementation in the approximate order in which it should be done. It also details optional features that you may or may not choose to implement. As the options are discussed, links to additional information are provided.

Before implementing endpoint compliance, it is recommended that you notify all users about your network usage requirements. This helps users anticipate the changes and reduces calls to your IT Staff.

Agent

Choose one or more agents

The first step in implementing endpoint compliance is determining whether you will use the Persistent Agent, the Dissolvable Agent, the Passive Agent, the Mobile Agent or a combination.

- The Persistent Agent is installed on the host and remains there to scan the computer as needed.
- The Dissolvable Agent is downloaded to the host and removes itself once the host has passed the security scan. If the host does not pass the scan, the Dissolvable Agent remains on the host for the user to run again after compliance issues have been resolved.
- The Passive Agent is provided using an external method, such as Group Policy Objects, and launched when the user logs into the domain. Users experience a slight delay while logging in but are unaware that their hosts are being scanned. See [Passive Agent on page 604](#).
- The Mobile Agent is installed on Android devices and is downloaded from either the captive portal or Google Play.

You may have situations in which one agent works better than others. For example, network users who log into your network every day could use the Persistent Agent and guest users could use the Dissolvable Agent. See [Agent overview on page 492](#) for additional information.

Use the latest agents

You may not have the most recent version of the selected agent on your FortiNAC appliance. Use the Agent Distribution window to see which agents are installed. From this window download the latest agent from Fortinet, if you need it. See [Agent packages on page 992](#). Not all agent versions are compatible with all FortiNAC versions. It is recommended that you check with a sales or support representative before using a new agent.

Deploy selected agents

Once you have determined which agents to use, you must decide how to deploy them. Typically agents are deployed using the portal pages or web pages that users see when they connect to your network. These web pages allow users to download an agent and install it on their hosts. If this is the method you use to give the agent to your hosts, no special setup is required. FortiNAC takes care of making the agent available via its own web pages based on the options selected in the endpoint compliance policy. Go to the portal configuration window and edit the content displayed on those web pages in order to customize them. See [Content editor on page 632](#).

Deployment options for each agent are as follows:

- Dissolvable Agent: Can be deployed from the captive portal or a separate web page.
- Passive Agent: Deployed using an external method, such as group policy objects. This agent is launched and served to the host when the users logs onto the network.
- Mobile Agent: Deployed using the captive portal or Google Play.
- Persistent Agent: Deployed using the captive portal, a separate web page or some other software distribution method.
 - If you choose to deploy the agent outside of FortiNAC you must download the agent and make it available for your chosen distribution method. See [Agent packages on page 992](#) for information on downloading the latest agent.
 - Go to the Persistent Agent Settings to configure agent behavior and the server with which the agent must communicate. See [Persistent Agent on page 913](#).

Agent / server communications

All Agents must be configured to communicate with the FortiNAC server while they are scanning the host. The default configuration is for the agent to communicate based on the server alias "ns8200". To ensure that this communication is successful the alias must be resolvable through DNS. Agents distributed through the captive portal are set automatically to communicate with the server. Additional settings in both FortiNAC and your Production DNS direct the agent to the correct server. See and .

Agents at V3.0 or higher are designed to use a secure communication protocol with the FortiNAC Server or Application Server; however, that does require some configuration.

Endpoint compliance policy

When you have determined the agent or agents to be used, you are ready to begin configuring your endpoint compliance policy.

- Create user/host profiles to determine which users/hosts will match a policy. See [User/host profiles on page 466](#).
- Create endpoint compliance policy to evaluate the hosts connecting to your network. See [Policies on page 531](#).
- Policies contain Scans that rely on having up-to-date information about antivirus and operating systems. In order to ensure that you have the latest information at all times you should configure a schedule for and run the Auto Def Updates.
- If you plan to use custom scans, you must create them first and then associate them with a Scan. This can be done at any time you feel that a custom scan is necessary. New custom scans can be associated with existing Scans. See [Custom scans on page 560](#).
- For each Scan that you create, decide how often to rescan hosts assigned to that policy. Setup a rescan schedule. See [Schedule a scan on page 556](#).
- If you are using the Dissolvable Agent and you want to allow hosts to rescan at their convenience, enable Proactive scanning.
- When a host fails a scan the user sees a web page with a list of reasons for the failure. To comply with your organization's requirements, that host may need access to certain web sites. For example, if the host failed because virus definitions were not up to date, that host needs to access the antivirus software manufacturer's web page to download new virus definitions. FortiNAC has a list of web sites that are made accessible even when a host has failed a scan. Make sure that the web sites for the software you require are included in that list.
- To understand what determines the policy that is assigned to a host, see [Policy assignment on page 458](#).

Events & alarms

- Make sure the **Security Risk Host** event is enabled, so that an event is generated any time a host fails a scan. The event message provides you with information about the host and why they failed. This is optional, but may be helpful in troubleshooting. See [Enable and disable events on page 773](#).
- You can view the list of events that have been generated by going to the Events View. See [Events on page 749](#).
- If you would like to be notified that a host has failed a scan, map the **Security Risk Host** event to an alarm. Within the alarm configuration you can specify that you would like to be notified via email or you can use the Alarm Panel on the dashboard. This alarm notifies you when a host has failed a scan and helps you trouble shoot any problems. You can also set up e-mail notification for users so they are aware that their host failed a scan. See [Map events to alarms on page 784](#) and [Alarms on page 88](#).
- Make sure that your administrator e-mail address and your e-mail server have been configured or FortiNAC will not be able to send e-mail notifications. See [Email settings on page 937](#).

Ports - control access

- Place ports for wired switches in a Forced Registration group. This forces hosts connecting on those ports to the Registration VLAN and displays the registration page. From this page they can download an agent and be scanned. See and .
- Hosts who have an agent and have already registered are not forced to the registration page. They are sent directly to the network. They are rescanned based on the schedule you have implemented for their policy.
- If you have a Remediation or quarantine VLAN where hosts are placed when they fail a scan, you must place ports in a Forced Remediation group. Placing ports in this group enables the quarantine VLAN switching option. If you are not ready to begin placing hosts in Remediation, you can disable this option.
- When quarantine VLAN switching is disabled, hosts are scanned and can see the passed and failed items from their scans, but they are given access to the network instead of being put into the quarantine VLAN. This is a good option to use when testing out the system. See [Quarantine on page 908](#).
- Other groups you may choose to use are Forced authentication, Dead End and Role Based Access.

Scan hosts without enforcing remediation (optional)

To scan hosts without placing "at risk" hosts in remediation you can enable one or more options. See [Scan hosts without enforcing remediation on page 545](#) for more details.

- Disable quarantine VLAN switching to scan hosts but not mark them "at risk".
- Enable the Audit Only option on an endpoint compliance policy. Hosts that fail when scanned with that policy are not marked "at risk" .
- Add hosts to the Forced Remediation Exceptions Group. Hosts in this group are scanned with the policy that corresponds to them. Hosts that fail the scan are marked "at risk" but are not forced into remediation.

Delayed remediation for scanned hosts (optional)

Allows you to scan hosts, notify the users of hosts that fail the scan of any pending issues, but not place the host in Remediation for a specified number of days. See [Delayed remediation on page 546](#).

- Enable the Delayed Remediation setting on one or more endpoint compliance policies by entering the number of days for the delay.

Switches - model configuration

- Go to the Model Configuration for your wired and wireless switches and configure your VLANs. See [Model configuration on page 338](#).

Authentication

- If you are using the Persistent Agent, you must set the method for authenticating your users in the Credential Configuration and in portal configuration. The authentication method selected must be the same in both places. See [Credential configuration on page 918](#).
- If you are using the Dissolvable Agent or the Mobile Agent, you must set the method for authenticating your users in the portal configuration window.

Monitoring

- Use the Scan Results View to see a list of hosts with their current scan status. This view provides information on the Scan used and whether or not the host passed the scan. See [Scan results on page 804](#).
- Use Standard Reports to view lists of policies, the number of scans run that were passed or failed and details on the Pass/Fail. See [Standard report templates on page 793](#).
- Use the Health Tab under Host Properties to view detailed scan information for an individual host. See [Host health and scanning on page 224](#).

Testing

It is recommended that you spend considerable time testing your endpoint compliance policies, web pages and VLAN switching before fully implementing endpoint compliance. Use your own hosts and go through as many failure scenarios as possible to make sure that hosts are being managed correctly.

Agent overview

Agents are used to scan hosts and determine whether the host complies with the endpoint compliance policy assigned to that host. Agents can perform additional functions, such as installing a Supplicant Configuration for a secure network. Several types of agents are available with FortiNAC, the Dissolvable Agent, the Passive Agent, the Persistent Agent and the Mobile Agent.

When hosts are scanned by an agent and fail, there are several options:

- Administrators can simply receive a warning that the host has failed the scan along with a list of what the failures were, but the host is given access to the network.
- Users can receive a warning that they have failed and be given access to the network.
- The network can be configured to move failed hosts off the production VLAN into the quarantine or remediation VLAN. This happens regardless of the agent type being used. Once remediation has taken place and the host has passed the scan, the host is moved back to the production VLAN.

Custom scans using HKEY_CURRENT_USER or HKEY_CLASSES_ROOT may not behave the same with the Persistent Agent as they do with the Dissolvable Agent. If HKEY_CLASSES_ROOT exists in HKEY_LOCAL_MACHINE\Software\Classes, it should work the same for both agents.

If you experience any problems with your Multilanguage operating system, please contact TAC Support.

Dissolvable Agent

The Dissolvable Agent is downloaded to the host by the user. The user runs the agent and the agent scans the host. If the computer is compliant with the endpoint compliance policy used for the scan, it is allowed on the network and the agent removes itself from the computer. If the computer is not compliant with the endpoint compliance policy, the Dissolvable Agent remains on the host to be used in a future scan after compliance issues have been addressed.

This agent can run custom scans, verify that Hotfixes are installed, check for antivirus and antispyware and operating system information.

The Dissolvable Agent files are different for Windows, macOS, and Linux.

Passive Agent

The Passive Agent is not installed, but is served as the user logs onto the network and does a scan in the background. See [Passive Agent on page 604](#). This agent can run custom scans, verify that Hotfixes are installed, check for antivirus and antispyware and operating system information. This agent runs only on Windows.

Persistent Agent

The Persistent Agent can be downloaded to the host and installed by the user, by a login script or by any other software distribution method your organization might use. The Persistent Agent remains installed on the host at all times. Once the agent is installed it runs in the background and communicates with FortiNAC at intervals established by the FortiNAC administrator.

The Persistent Agent can be configured to provide messages to the user when the host is scanned indicating the results of the scan. In addition you can provide pop-up messages indicating the host's current state, such as disabled, requires authentication or network access is normal. See [Persistent Agent on page 913](#).

The Persistent Agent can run custom scans and monitors, verify that Hotfixes are installed, check for AntiVirus and AntiSpyware and operating system information and allow an administrator to send a message to the host.

Mobile Agent

The Mobile Agent is downloaded and installed either from the captive portal or from Google Play depending on device settings. The Mobile Agent assist with authentication and registration and provide an inventory of installed apps. The Mobile Agent can determine whether the device is rooted or not. A device is considered rooted when a user has accessed the secure areas of the operating system on the device.

Dissolvable Agent

The Dissolvable Agent is an application that works on Windows, macOS, or Linux hosts to identify them to FortiNAC. The agent scans them for compliance with an endpoint compliance policy. This agent is downloaded and installed on the host until the host passes the scan. The agent then removes itself.

In a Windows environment, there are some operations that the Dissolvable Agent cannot perform unless the user has administrator privileges on the PC, such as release and renew the IP address on the PC.

Setup requirements and options

- Make sure the latest Dissolvable Agent package is installed on the FortiNAC server.
- The Dissolvable Agent can be downloaded and installed by the user through the captive portal. The portal itself can be modified and personalized. Dissolvable Agent also has some settings in the portal under **Agent > Dissolvable**. See [Portal configuration on page 631](#).
- If you are using the Dissolvable Agent, the FortiNAC appliance must be configured with SSL and must have a valid third party SSL certificate from a CA. A self-signed certificate cannot be used.
- Dissolvable Agent discovers the server to which it should connect using DNS SRV records. If for any reason, it cannot discover the server, the user is presented with an option to enter either the URL or the FQDN of the server. The URL field will accept an HTTPS address, the FQDN of the server which it uses to create an HTTPS address or an HTTP address. If an HTTP address is used, a warning is displayed asking the user to confirm that they wish to access the server over an insecure connection. Depending on your configuration you may need to supply this information to users running the Dissolvable Agent.

Using the Dissolvable Agent

If you have chosen to use the Dissolvable Agent to scan Windows or macOS systems, the Dissolvable Agent is downloaded to the host. Once the Dissolvable Agent runs and the host has successfully passed the scan, the agent is removed from the host.

In a Windows environment, there are some operations that the Dissolvable Agent cannot perform unless the user has administrator privileges on the PC, such as release and renew the IP address on the PC.

Registration

When an unknown host connects to the network and attempts to access the Internet, an entry in the DNS server redirects the host to the Login page for registration.

During registration FortiNAC determines which endpoint compliance policy should be applied to this host based on the user/host profile that the connecting user and host match.

Endpoint compliance policies contain a series of requirements for hosts that want to access the network. Endpoint compliance policies contain scans that are configured by the Administrator and are run by the Agent. Policy requirements can include scans for specific antivirus, operating system version and custom scans. Custom scans are created by the Administrator. These allow the administrator to scan for the existence of things such as a specific file, a registry entry, an installer package, a specific process or a domain.

The endpoint compliance policy determines which agent is made available to the user for download, such as Dissolvable Agent or Persistent Agent.

Hosts connecting to the network will go through the process outlined below:

1. User connects to the network and is placed in registration. The registration web page is displayed.
2. User downloads the Dissolvable Agent to the default downloads location for the operating system.
3. Run the downloaded file and install it on the device.
4. After the Dissolvable Agent is installed, run the program. An Agent window is displayed and remains on the screen until the user closes it.
5. The Dissolvable Agent uses the DNS SRV records to locate the appropriate FortiNAC server.
6. If the Dissolvable Agent cannot locate the server, a message is displayed asking for the URL of the server. The user is presented with an option to enter either the URL or the FQDN of the server. The URL field will accept an HTTPS address, the FQDN of the server which it uses to create an HTTPS address or an HTTP address. If an HTTP

address is used, a warning is displayed asking the user to confirm that they wish to access the server over an insecure connection.

7. The Agent window displays the results of the scan.
8. If the host fails scan, **Rescan** is displayed allowing the user to Rescan after correcting any issues.
9. When the host passes the scan, the user closes the Agent window and the Dissolvable Agent dissolves.

Persistent Agent

The Persistent Agent is an application that works on Windows, macOS, or Linux hosts to identify them to FortiNAC and scan them for compliance with an endpoint compliance policy. This Agent is downloaded and installed on the host permanently.

Communication

The Persistent Agent installed on a host is designed to "check in" through a periodic heartbeat sent to the Persistent Agent server. This lets the server know that the Persistent Agent is still installed and running on the host. When this does not happen, a "Lost Contact with Persistent Agent" event is generated indicating that the server cannot communicate with the host. When the Persistent Agent eventually contacts the server again a "Regained Contact with Persistent Agent" event is generated.

Lost contact with the Persistent Agent is intended to communicate to FortiNAC Administrators that hosts that are marked as having the Persistent Agent are online and not communicating to the FortiNAC agent server. Lost contact with the Persistent Agent detection can take up to approximately 90 minutes from the first failure to communicate detection to generate the Event. This also depends on the L2 poll interval of the Network Device.

The Persistent Agent communicates using the following ports:

- tcp 4568
- tcp 80 (required for upgrades)



The "Lost Contact with Persistent Agent" event only detects that the agent is no longer successfully communicating. This loss of contact could be caused by many things including: a missing or disabled agent, a lack of network connectivity, a lack of network activity that would prevent FortiNAC from polling to discover that the host was offline, a firewall that prevents communication between the agent and the server or any other issue that would interrupt communication.

The Persistent Agent does work within the context of FortiNAC's VPN integration.

Setup requirements and options

- FortiNAC-OS Requirement: "nac-agent" and "http" options must be included in the "set allowaccess" command. See [Open ports](#) for details.
- Make sure the latest Agent package is installed on the FortiNAC server.
- Add SRV records to your production DNS server that allow the agent to locate the FortiNAC Server or Application server to which it should connect.
- If you are using Persistent Agent 3.X or higher, the FortiNAC appliance must be configured with SSL and must have a valid third party SSL certificate from a CA. A self-signed certificate cannot be used.
- The 3.x Persistent Agent communication method requires not only SSL certificates be installed for the Persistent

Agent target in FortiNAC, but also the root certificate be installed on the endstation hosting the agent. The Persistent Agent reads all certificates from the trusted root certification authorities store of the system account. If the CA is not listed in this store, the Persistent Agent will not trust the connection to FortiNAC and will not communicate.

FortiNAC does not push root certificates to endstations. Root certificates come pre-installed with the host's operating system. Any additions or updates to root certificates are distributed via the host's OS updates.

- The Persistent Agent can be downloaded and installed by the user through the captive portal, by a login script or by any other software distribution method your organization might use. Determine your distribution method.
- If you plan to deliver the agent via the captive portal, configure the portal styles. See [Portal configuration on page 631](#).
- You can configure FortiNAC to authenticate users with their Windows domain logon credentials eliminating the need for the Persistent Agent to ask for credentials. See [Using Windows domain logon credentials on page 502](#).
- The Persistent Agent can be configured to provide messages to the user when the host is scanned indicating the results of the scan. In addition you can provide pop-up messages indicating the host's current state, such as disabled, requires authentication or network access is normal. See [Persistent Agent on page 913](#).
- In addition to the settings contained within the admin UI, registry settings on Windows hosts can be configured using Group Policy Objects. These registry settings contain the URL of the FortiNAC Application Server, enable and disable the system tray icon or Balloon Notifications and various security settings. See [Agent packages on page 992](#).
- The Persistent Agent has different files for macOS and Windows operating systems. FortiNAC can be configured to update the Persistent Agent automatically with a user-specified version or an updated agent can be pushed to a specific host.
- The Persistent Agent can be used to apply a supplicant configuration to a host. See [Supplicant EasyConnect on page 595](#).

Host requirements and options

- The host must be running Windows, macOS, or Linux. Refer to the Agent Comparison table in [Agent overview on page 492](#) or the Release Notes for more detailed information about operating system versions that are supported.
- If the host is running a Virtual Machine (VM) with the Persistent Agent inside the VM, the VM must be bridged. The Persistent Agent is not fully functional when it runs in a NATed Virtual Machine on a host. The agent can contact the FortiNAC server and receive a response. However, unsolicited messages from the FortiNAC server fail to reach the agent.
- For the Persistent Agent to detect guest VMs running on the host, the VMs must be bridged. The VM adapters will then be associated with the host with the Medium of VirtualGuest.
- If the Persistent Agent is delivered via the captive portal, the user must install it manually. See [Installation for Windows on page 496](#) and [Installation for macOS on page 498](#).
- For an overview of the host registration and scanning process using the Persistent Agent, refer to [Using the Persistent Agent on page 501](#).

Troubleshooting

- If you are troubleshooting an issue with the Persistent Agent, review the logs generated on the host. See [Logging on page 505](#).

Installation for Windows

When a new host connects to the network, it is directed to a special web page that allows the user to download the Persistent Agent. Once the Persistent Agent has been downloaded, it must be installed on the host.

The Persistent Agent can also be delivered as an .msi file. This allows it to be pushed automatically from Active Directory.

Install

1. On the host, locate `Persistent Agent.exe` file that was downloaded. Double-click the to begin the installation process.
2. The Welcome window displays. Click **Next** to continue.
3. A progress window appears showing the status of the installation. The Installation Complete window displays.
4. Click **Finish**.
5. The Agent Icon appears in the system tray on the right.



Several right click options are available:

Option	Description
About	Displays the agent version, copyright, and other information.
Show Messages	Displays the list of the messages sent through the Persistent Agent that have been received by the host. If any URLs have been sent separate from a message, a list of these are also be displayed.
Login	Appears when host is in isolation requiring registration or authentication. When selected, opens a login dialog.
Log off the Network	Appears when host is logged in and authenticated. When selected, the host is logged off the network and is placed into isolation requiring authentication.
Show Network Access Status	Appears when the host is isolated for remediation or being disabled. When selected, the user is sent to either the remediation page for rescan or the dead end page if disabled.

6. The Agent automatically communicates with the FortiNAC Application Server to authenticate the user credentials.
7. Enter **User Name** and **Password**, then click **OK**. The user is authenticated and registered.

Note: For installing on Windows Servers, if the installation fails because of missing DLL, go to Windows Server Manager and install Wireless Lan Service to install the missing DLL.

Host firewall

When a host is running a Windows Firewall, the Persistent Agent automatically adds a program exception for itself to the Windows Firewall configuration. This is added to the currently active user profile, unless the "Domain" profile is active. For hosts using a different firewall you must meet the following requirements:

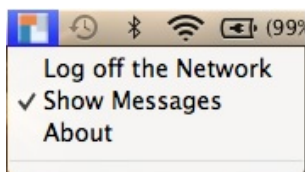
- An exception for the Persistent Agent must be added to the firewall
- TCP port 4568 must be available for agent communication

Installation for macOS

When a new host connects to the network, it is directed to a special web page that allows the user to download the Persistent Agent. Once the Persistent Agent has been downloaded it must be installed on the host.

Install

1. On the host, locate and open the **Persistent Agent.dmg** folder that was downloaded.
2. Double-click the **Persistent Agent.pkg** on the desktop to begin the installation process. Then click **Continue** to start the installation.
3. Select the drive where the Persistent Agent is to be installed, then click **Continue**.
4. Click **Install** to begin the installation of the agent on the local host.
5. Enter the local host's **administrator credentials** and click **OK**.
6. Click **Close** when the installation is complete.
7. Go to the desktop and unmount the Persistent Agent Installer by dragging it to the trash bin. The trash bin icon turns into an eject icon.
8. The Persistent Agent Icon appears in the system tray on the right. Click options for the icon are About and Show Messages.



Several options are available when you click the icon:

Option	Description
About	Displays the agent version, copyright, and other information.
Show Messages	Displays the list of the messages sent through the Persistent Agent that have been received by the host. If any URLs have been sent separate from a message, a list of these are also be displayed.
Login	Appears when host is in isolation requiring registration or authentication. When selected, opens a login dialog.
Log off the Network	Appears when host is logged in and authenticated. When selected, the host is logged off the network and is placed into isolation requiring authentication.
Show Network Access Status	Appears when the host is isolated for remediation or being disabled. When selected, the user is sent to either the remediation page for rescan or the dead end page if disabled.

9. The Agent automatically communicates with the FortiNAC Application Server to authenticate the user's credentials. Enter **User Name** and **Password**, then click **OK**. The user is authenticated and registered.

If the Agent will not run (e.g., there is no icon displayed), uninstall the PA and run the following command from the command line (Terminal). Then, re-install the PA.

```
sudo /usr/sbin/pkgutil --forget com.bradfordnetworks.PersistentAgent
```

Uninstall

Go to */Library/Application Support/Bradford Networks/Persistent Agent/Uninstall*

Installation for Linux

When a host connects to the network, it is directed to a special web page that allows the user to download a rpm or deb package of the Persistent Agent. Once the Persistent Agent has been downloaded, it must be installed on the host.

Considerations

Some AntiVirus products on Linux need extra permissions for the Agent to access them. If the AntiVirus program is installed after installing the agent, those permissions will not be set. The scans for the newly installed programs will not work as expected.

Use the following command on the host machine to restart the agent service (bndaemon):

```
sudo service bndaemon restart
```

The following AntiVirus programs require a restart of the agent service if installed after the FortiNAC Persistent Agent:

Sophos SPL

CrowdStrike falcon

Install

1. On the host, locate the directory where the rpm or deb agent package was downloaded.

Package filename convention (Pre- Agent 7.6):

```
fortinac-persistent-agent_XX.X.X.XX-X.x86_64.rpm
```

```
fortinac-persistent-agent_XX.X.X.XX-X.amd64.deb
```

Package filename convention (Agent 7.6 +):

```
fortinac-agent_XX.X.X.XX-X.x86_64.rpm
```

```
fortinac-agent_XX.X.X.XX-X.amd64.deb
```

2. Refer to the table below for commands to install the Persistent Agent package.

The following commands are run on the host:

Package Extension	Install Command
Rpm	\$ sudo rpm -Uvh <agent package .rpm filename>
Deb	\$ sudo dpkg -i <agent package .deb filename>



3. The Persistent Agent Icon appears in the tool tray.
Several options are available when selecting the icon:

Option	Description
About	Displays the agent version, copyright, and other information.
Show Messages	Displays the list of the messages sent through the Persistent Agent that have been received by the host.

Option	Description
	If any URLs have been sent separate from a message, a list of these are also be displayed.
Login	Appears when host is in isolation requiring registration or authentication. When selected, opens a login dialog.
Log off the Network	Appears when host is logged in and authenticated. When selected, the host is logged off the network and is placed into isolation requiring authentication.
Show Network Access Status	Appears when the host is isolated for remediation or being disabled. When selected, the user is sent to either the remediation page for rescan or the dead end page if disabled.

- The Agent automatically communicates with the FortiNAC Application Server to authenticate the user's credentials. Enter the User Name and Password, then click **OK**.
The user is authenticated and registered.

If FortiNAC's DNS does not contain the specific SRV records used by the Persistent Agent to locate the server, the end user must run the setup script to edit the configuration file for the Linux Persistent Agent.

To run the setup script, do the following:

- To stop the Linux Persistent Agent service type: `$ sudo service bndaemon stop`
- Run the setup script.
 - Type `$ cd /opt/com.bradfordnetworks/PersistentAgent`
 - Type `$ sudo ./setup`
 - Enter the following configuration values from the setup:
 - Home Server: Enter the FQDN of your the FortiNAC Application Server
 - Allowed Servers: Enter any other FortiNAC servers the Agent would need to communicate with.
 - Restrict roaming: Restrict the agent to only communicate with servers listed in the Home Server and Allowed Servers fields.
- To start the Linux Persistent Agent service type: `$ sudo service bndaemon start`

Right-click options

Option	Description
About	Displays the agent version, copyright, and other information.
Show Messages	Displays the list of the messages sent through the Persistent Agent that have been received by the host. If any URLs have been sent separate from a message, a list of these are also be displayed.
Login	Appears when host is in isolation requiring registration or authentication. When selected, opens a login dialog.
Log off the Network	Appears when host is logged in and authenticated. When selected, the host is logged off the network and is placed into isolation requiring authentication.
Show Network Access Status	Appears when the host is isolated for remediation or being disabled. When selected, the user is sent to either the remediation page for rescan or the dead end page if disabled.

Host firewall

When a host is running a firewall (iptables), the Persistent Agent will need the port 4568 open in order to communicate with FortiNAC.

Uninstall

Refer to the table below for commands to uninstall the Persistent Agent package.

The following commands are run on the host.

Agent Version	Uninstall Command
Pre- Agent 7.6	<pre>rpm: \$ sudo rpm -ev fortinac-persistent-agent deb: \$ sudo dpkg --purge fortinac-persistent-agent</pre>
Agent 7.6 +	<pre>rpm: \$ sudo rpm -ev fortinac-agent deb: \$ sudo dpkg --purge fortinac-agent</pre>

Using the Persistent Agent

If you have chosen to use the Persistent Agent to scan Windows, macOS, or Linux systems, hosts connecting to the network will go through the following process. The PA is downloaded to the host and installed. Once PA is installed it runs in the background and communicates with FortiNAC at intervals established by the network administrator.

The Persistent Agent will not detect the addition of a guest to a virtual host record unless the "Append to Host" or "Register as New Host" options are enabled in the VM Detection settings, and the port they are connected to may be subject to isolation and registration policies. See [Properties on page 919](#).

Registration

When an unknown host connects to the network and attempts to access the Internet, an entry in the DNS server redirects the host to the Login page for registration.

The Persistent Agent can also be used to register hosts passively (behind the scenes).

To begin the registration and policy check process, the user on the unknown host does the following:

1. Enter the User Name.
2. Enter the Password.
3. Click Download.
4. Save the file to the Desktop as directed by the browser download functionality or runs the file.

If a Persistent Agent is being used, the host must install the Persistent Agent the first time. If a Dissolvable Agent is being used, the agent runs without installing any files.

Results

Once the security check has completed, if the host failed to meet the security policy, a results page shown in a browser lists the items that failed and passed.

You can configure a link that the user can click that provides information about items that failed and what to do to correct the problem. Enter this link when you configure the policy. See [Add or modify a scan on page 547](#) for more information.

If you do not provide a link, modify the failure page to provide information for the user to correct the problem and find assistance.

Rescan

Once the user has corrected any issue(s) that caused the failure, the Persistent Agent security check must be run again.

1. Open a browser window.
2. Host is placed in Remediation.
3. Click on the link associated with the security policy.
4. Click Rescan.

This process may need to be completed again if additional issues remain that cause the host to fail the security policy.

Successfully registered notification

Once all the items causing the host to fail the security policy have been corrected, the host is registered and the Success message window is displayed.

Using Windows domain logon credentials

With the Persistent Agent, you can configure FortiNAC to authenticate users with their Windows domain logon credentials eliminating the need for the Persistent Agent to ask for credentials. You must use Active Directory and Group Policy Objects to manage your Windows hosts. To implement this feature your system must meet the following requirements:

- **Active Directory:** You must be using Active Directory to authenticate users. The directory must be configured in **System > Settings > Authentication > LDAP**. See [Directories on page 868](#) for configuration information.
- **Authentication:** In **Policy & Objects**. Under **Authentication**, click **Configuration**. Click **Add**, or select a configuration and click **Modify**. Make sure that **Enable Authentication** is selected.
- **Passive Agent Configuration:** At least one Passive Agent rule or configuration must be set up. The Persistent Agent uses this configuration to process session notification information from the host. Navigate to **Policy & Objects > Passive Agent**. Add a configuration that is enabled and that applies to a directory group that contains all the users for whom this feature is being implemented. If you plan to have the Persistent Agent register hosts as devices, you must also include that setting in the Passive Agent configuration you are creating.
- **Persistent Agent Properties:** Navigate to **System > Settings > Persistent Agent**. Under **Status Notifications**, disable the **Provide a Log Off functionality from the tray icon for authenticated hosts** option. This can remain enabled; however, if the user were to log off using the Persistent Agent icon, the host would be automatically logged on again the next time the server requests credentials. If you plan to have the Persistent Agent register hosts as devices, click the **Credential Configuration** tab and enable the **Register as Device** option.

If you want to prevent users from being able to log off the network using the Agent Icon you must also disable the display a special "Needs to Authenticate" icon when a host needs to authenticate option on the **Status Notification** tab. This is optional, not required.

- **GPO Templates:** Download and install the latest Persistent Agent Administrative Templates.

After installing the templates on your Windows server you must modify the following Persistent Agent Template settings:

- **Host Name:** Ensures that the Persistent Agent is communicating with the correct FortiNAC server.
- **Login Dialog:** Allows you to enable or disable the Login dialog that is presented by the Persistent Agent during authentication. Disable the Login dialog to use the users' Windows login credentials.

GPO settings for high availability



If you are using Persistent Agent version 3.X or higher, this issue does not apply.

For the Persistent Agent to communicate with a FortiNAC appliance the agent must know the name or IP address of that appliance. Group Policy Objects can leverage templates distributed by Fortinet to modify the host registry and provide the Persistent Agent with the hostname of the FortiNAC appliance. However, in a high availability environment, the agent must also know how to communicate with the secondary server in the event of a failover.

High availability or redundant servers can be set up in two ways. In an L2 or single subnet configuration, the FortiNAC servers share a virtual IP address and server name. In a failover situation, the transition is seamless because agents continue to communicate with the same virtual IP address or name no matter which FortiNAC appliance is in control. In an L3 environment where redundant servers are on different subnets, there is no shared IP address. The agent must know how to connect to both servers.

If you are running in a high availability environment, you must analyze the HA configuration, the version number of the agent being used and the method used to establish communication between the FortiNAC appliance and the Persistent Agent. You may need to alter the way you inform the Persistent Agent of the server name or IP address.

When a template is served to a host, the template writes to the following keys in the Windows registry:

- HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Bradford Networks\Persistent Agent
- HKEY_LOCAL_MACHINE\SOFTWARE\Bradford Networks\Client Security Agent

The Persistent Agent key takes precedence over the Client Security Agent key. However, in an L3 environment with redundant servers on different subnets, if there is a fail over, FortiNAC can only update the value in the Client Security Agent key. Since the Persistent Agent key takes precedence, the agent does not communicate with the correct server.

The sections below provide an overview of successful configuration combinations for Persistent Agent / Server communication in a high availability environment. This is particularly important when hosts are configured using templates served by Group Policy Objects to modify the host registry.

L2 high availability

In this environment, redundant servers share a virtual IP address and a server name. To configure communication between the agent and the FortiNAC server, navigate to **System > Settings > Passive Agent > Properties**, and set Primary and Secondary Host Name using the FortiNAC Server/Application Server Fully Qualified Domain Names. For more details, refer to [High Availability](#) document.

L3 high availability

In this environment, redundant servers are on different subnets and have different IP addresses. In this scenario, there is only one option.

You can use GPO to deliver a template to the host where the Persistent Agent is installed; however, you must NOT configure ServerIP in the template. It is important that the associated registry keys not be configured on the host.

You must navigate to **System > Settings > Passive Agent > Properties**. Add the server name of both the primary and secondary FortiNAC servers.

In the event of a failover, the name of the secondary FortiNAC server is pushed to the Persistent Agent.

Certificate validation

The Persistent Agent can be configured using a Windows custom scan to validate the certificate on a host against the certificate provided by the administrator on Active Directory.

The application server must have access to the web server.

The certificate check custom scan allows the Persistent Agent to verify whether the certificate on the host matches the certificate on the network. The Persistent Agent scans the host and sends the timestamp, client certificate, and signature to the server. The server then completes the following process:

- Validates the certificate against a trusted CA that is provided by the administrator
- Verifies the revocation against the CRL (certificate Revocation List) provided through the LDAP or web server.
- Verifies the timestamp is within five minutes of receipt by the server.
- Verifies the signature with the certificate's public key.
- Updates the scan result to change the default failure state to success, and updates the overall result from failure to success, if necessary.

Implementation

1. Upload and install the certificate from a trusted CA for validation by the server, and select **Persistent Agent Cert Check** as the target. See [SSL certificates on page 509](#).
2. Create a Windows certificate check custom scan to verify the certificate on the host. See [Windows Custom Scan on page 570](#).
3. Add the certificate check custom scan to a scan that is enabled within your endpoint compliance policy. See [Create a scan on page 561](#).

Upgrade the Persistent Agent

Global update

Hosts on your network that have a Persistent Agent installed can be updated automatically using the settings in **System > Settings > Persistent Agent > Agent Update**. See [Agent update on page 913](#) for instructions.

Update on a single host

Hosts on your network that already have a version of the Persistent Agent installed can be updated individually. The FortiNAC administrator may choose to selectively update a few hosts to test a new version of the Agent or to install an earlier version of the agent on an older host.



Clients upgrading the Persistent Agent must have access to Port 80 on the FortiNAC appliances.



The update is sent immediately to the host. The host must be running and connected to the network for the update to be successful.



If the host has software installed to reset the host to its original configuration after a re-boot, the agent reverts to the previous version. The software must be disabled before updating the Agent.

A special group, **Global Agent Update Exceptions**, has been created to stop selected hosts from being automatically updated. Any host in this group is not updated. If you update a host to an agent version that is different from the version selected for Global Agent Updates, this host is automatically moved to the Global Agent Update Exceptions Group. If necessary, this host must be manually removed from that group. See [Group membership on page 231](#) for instructions.

To select and update a host:

1. Click **Users & Hosts > Hosts**.
2. Right-click on the host and select **Host Properties**.
3. A window displays containing the host information. If the host has more than one MAC address, all are displayed.
4. In the Policy Agent/Access section of the window, locate the **Agent Version** field. The agent version that is currently installed on the host is displayed.
5. Click **Update**.
6. Select the new Persistent Agent version from the drop-down list and click **OK**.

When you select **OK**, FortiNAC “polls” the host to determine the point at which the version number changes to the new version. This “polling” times out after a minute or when the new version number is returned. If the update times out without returning a new version number, a message that the update has failed is displayed. If the new version number is returned, a message that the update was successful is displayed.



No events are generated based on the success or failure of an individual host update.

Logging

The Persistent Agent has a logging feature for packet activity on the host. The log file automatically rotates every 24 hours based on the installation time of the Persistent Agent. The log file is stored in the following locations:

Windows

For Windows Operating systems look in the Common Application Data directory at %ProgramData%\Bradford Networks\

macOS

For macOS log messages are sent to the system log via the "debug" syslog priority.

- On 10.5 and 10.6 messages show up in `system.log`
- On 10.4 these messages show up in `console.log`

Linux

- On Linux (Debian Based), these messages show up in `/var/log/syslog`
- On Linux (Red Hat Based), these messages show up in `/var/log/messages`



Time stamps included in the log file are displayed in UTC time. Coordinated Universal Time (UTC) is a high precision atomic time standard that corresponds roughly to Greenwich Mean Time.

Mobile Agent

Mobile Agent is an application that works on Android devices to identify them to FortiNAC, assist with authentication and provide an inventory of installed Apps. The Mobile Agent can scan the device for indicators of rooting. Rooting is a process allowing users of devices running the Android operating system to attain privileged control (known as "root access") within Android's subsystem.

FortiNAC will only require or respond to a Mobile Agent if the Policy that applies to the host includes settings requiring the Mobile Agent. If for any reason a mobile device had a Mobile Agent installed, the user would not be able to register the device unless the policy assigned included the Mobile Agent. If the policy assigned is set to None-Deny, the mobile device is not allowed to register. If the policy is set to None-Bypass, the mobile device can be registered but not using the installed Mobile Agent.

The Mobile Agent does work within the context of FortiNAC's VPN integration.

Setup Requirements

- Make sure the latest Agent package is installed on FortiNAC.
- Add SRV records to your production DNS server that allow the agent to locate the FortiNAC Server or Application server to which it should connect.
- The Mobile device must be running Android operating system 2.3.3 or higher.
- Users can download the agent one of two ways:
 - If the Android device is configured to allow downloads from unknown sources, the Mobile Agent can be downloaded from the captive portal. For example, configure an Android phone by choosing Settings from a Home screen, then selecting Applications and enabling the Unknown Sources option.
 - If the Android device does not allow downloads from unknown sources, the Mobile Agent must be downloaded through Google Play.
- FortiNAC appliance must be configured with SSL and must have a valid third party SSL certificate from a CA. A self-signed certificate cannot be used. See [Agent server communications on page 507](#).
- Create an endpoint compliance policy for Android devices to control whether or not an agent is required and whether or not the device can register. See [Policies on page 531](#).
- To prevent Rooted devices from registering, enable Root Detection in the Scans used for Mobile devices. See [Add or modify a scan on page 547](#). When Root Detection is not enabled, the Mobile Agent still determines whether the device is rooted, but allows the device to register and appends (Rooted) to the operating system information displayed in the Host View.



Root Detection happens only during registration. If a user registers a device and then later alters that device causing it to be Rooted, FortiNAC is not notified. You may want to age these devices out of the database quickly so the user is forced to re-register periodically.

- Enable the **Potential Rooted Device** event and alarm to be notified when the Mobile Agent determines that the devices may be rooted. The event message contains the username of the user and the MAC addresses of the device. See [Enable and disable events on page 773](#).
- Mobile device users are authenticated based on the settings for standard user login. Navigate to **Portal > Portal Configuration > Content Editor**. In the tree on the left select **Global > Settings** and verify that the **Standard User Login Type** is correct.
- You can modify the default text shown in the captive portal as mobile device users connect to the network. Navigate to **Portal > Portal Configuration > Content Editor**. In the tree on the left scroll to the **Registration > Mobile Agent Download** section to review or modify the download page. In the tree on the left, scroll to the **Agent > Mobile** section to review or modify the Login page.

Notes

- If the Mobile device attempts to connect to the network but never reaches the agent download page and is never prompted for credentials, verify that the device is receiving an IP address within the Registration VLAN. Verify that the device is connected to the correct SSID.
- If the user receives a message indicating that they do not have rights to access the network, verify that there is a Policy in place for mobile devices and that it is configured correctly.

Agent server communications



FortiNAC-OS Requirement: "nac-agent" and "http" options must be included in the "set allowaccess" command. See [Open ports](#) for details.

The sections below provide instructions for securing communications between the agent and the FortiNAC server with a trusted SSL certificate, setting up communication between the agent and the server, and the host registry settings or preferences that can be modified to customize Persistent Agent behavior.

Implementation

Update FortiNAC

Requires FortiNAC version 5.3.3 or higher to enable security.

You must have the latest Auto-Definition files installed. See [Auto-definition updates on page 531](#).

Certificates

You must have a separate certificate for each FortiNAC server that runs the captive portal, such as the FortiNAC Application server or the stand-alone FortiNAC Server.

Certificates must be from a trusted certificate authority (CA), such as VeriSign, Thawte, or GeoTrust.

Self-signed certificates are not recommended. If you use a self-signed certificate, end users will receive constant pop-up warnings indicating that the site is not secure and asking them to confirm that they wish to continue. In addition, the Mobile Agent absolutely require a certificate from a trusted CA. The Mobile Agent cannot communicate with FortiNAC when Self-signed certificates are used.

If you already have a certificate that you are using to secure your portal, you can import that certificate into the FortiNAC server configuration and use it for both the portal and agent/server communications.

If you do not have a certificate for your portal, generate a certificate request and purchase a certificate. When the certificate is returned, import that certificate into the FortiNAC server configuration and use it for both the portal and agent/server communications.

Persistent Agent, Dissolvable Agent, and the Mobile Agent require the use of a certificate.

The 3.x Persistent Agent communication method requires not only SSL certificates be installed for the Persistent Agent target in FortiNAC, but also the root certificate be installed on the endstation hosting the agent. The Persistent Agent reads all certificates from the trusted root certification authorities store of the system account. If the CA is not listed in this store, the Persistent Agent will not trust the connection to FortiNAC and will not communicate.

FortiNAC does not push root certificates to endstations. Root certificates come pre-installed with the host's operating system. Any additions or updates to root certificates are distributed via the host's OS updates.

For instructions on generating and installing SSL certificates, see the document entitled **FortiNAC SSL Certificates How To**.

DNS server configuration

If you use agents for macOS and some Linux systems, using a .local suffix in **Domain** fields in the Configuration Wizard may cause communications issues.

Example:

Incorrect DNS suffix for reg: `tech-reg.megatech.local`

Correct DNS suffix for reg: `tech.megatech-reg.edu`

- On upgrade to V6.0 or higher, SRV records indicating the port and FQDN of the FortiNAC appliance where the portal is located are automatically added to the `domain.zone.*` files for named. These files are created by the Configuration Wizard, which can also add the SRV records to the `domain.zone.*` files during the initial appliance configuration.
- If you are unable to configure the agent through Agent Configuration, the same SRV records may be added to the corporate production DNS servers. Agents can then query the DNS servers to determine the FortiNAC server with which they should communicate.
- Any references to the FortiNAC server's FQDN in DNS must match the name in the certificate used to secure the portal.

See [DNS server configuration on page 514](#) and [Agent server discovery on page 519](#).

Server configuration



If the time on FortiNAC is inaccurate and is updated after Agent Security is enabled, Agents may ignore packets received from the server until the agent is restarted because the new timestamp deviates significantly from previous timestamps.

Make sure that the server is configured to use NTP for time synchronization. Go to **System > Settings > System Management > NTP and Time Zone** to configure the NTP server. This is typically set during installation.

Host configuration

- Host machines should not have the FQDN of the FortiNAC Server or Application Server in the hosts file on the hard drive. Typically network users would not have this information in their hosts file. However, administrator users may have the FQDN in their hosts file to accommodate accessing java applets. Modify the hosts file to use the short name, such as qa233 instead of qa233.example.com. If a host has the FQDN in its hosts file, the Persistent Agent cannot communicate with the FortiNAC Server or Application Server and cannot register the host.
- For Windows hosts, download and configure Administrative Templates for Group Policy Objects to update the registry on each host with values that pertain to agent security.
- For macOS hosts, update Preferences to provide security values to the agent.

See [Persistent Agent on Windows on page 521](#).

SSL certificates

The following components of FortiNAC are able to utilize SSL certificates for encrypting communications:

- **Administrator interface:** browser traffic between user managing FortiNAC through the UI and the FortiNAC Server.
- **Persistent Agent:** traffic between Persistent Agent (PA) installed on a host and the FortiNAC Application Server. Functions that utilize this communication include, but are not limited to, registration/authentication and scanning.
- **Portal:** browser traffic between host in isolation using the captive portal (Registration, Remediation, authentication, Dead End) and the FortiNAC Application Server. This is also used for traffic between the Dissolvable Agent, Mobile Agent, and the FortiNAC Application Server.

These components are secured independently of each other. However, the same SSL certificate can be used if multiple components are to be secured.

The following sections describe how to obtain, upload, and renew SSL certificates.

Implementation considerations

If you are running a high availability (HA) configuration using a shared IP address, the certificate information for the Portal target is replicated from the primary server to the secondary server. If you are running a HA configuration where primary and secondary servers are on separate subnets (L3 HA) contact Support for assistance.

You may act as your own CA and use your own internal certificate, as long as all systems in your domain use the same certificate.

The Persistent Agent and Dissolvable Agent cannot use the self-signed certificate.

Wildcard certificates

Wildcard certificates may be imported to secure the Captive Portal. They can either be generated from a certificate signing (CSR) created via FortiNAC or a third party.

To generate a wildcard CSR using FortiNAC, see [Obtaining an SSL certificate from a CA on page 510](#).

To use a wildcard certificate already generated, proceed to [Upload a certificate received from the CA on page 512](#).

Ensure the following when importing a wildcard certificate:

- The wildcard private key cannot be password protected.
- The actual fully qualified hostname must be entered in the fully qualified hostname Field in the General tab under **Go > Tasks > Portal Configuration**. Entering the wildcard name in this field will cause the application of the certificate to fail.

Subject Alternative Name (SAN) certificates

A SAN certificate can be used to secure multiple hostnames and/or IP addresses. For example, in a Layer 2 HA environment the virtual, primary, and secondary appliance hostnames and their corresponding IP addresses can all be secured with one certificate.

To generate a SAN certificate using FortiNAC, see [Obtaining an SSL certificate from a CA on page 510](#).

Create a keystore for LDAP

If you choose to use SSL or TLS security protocols for communications with your LDAP directory, you must have a security certificate. You must obtain a valid certificate from a certificate Authority. That certificate must be saved to a specific directory on your FortiNAC.

SSL or TLS protocols are selected on the **Directory Configuration** window when you set up the connection to your LDAP directory. Follow the steps below to import your certificate. You should be logged in as root to follow this procedure.

1. When you have received your certificate from the certificate Authority, copy the file to the `/home/admin` directory on your FortiNAC server.
2. Use the keytool command to import the certificate into a keystore file.

For example, if your certificate file is named `MainCertificate.der`, you would type the following:

```
keytool -import -trustcacerts -alias <MyLDAP> -file  
/home/admin/MainCertificate.der -keystore /bsc/campusMgr/.keystore
```



Depending on the file extension of your certificate file, you may need to modify the command shown above. For additional information on using the keytool key and certificate management tool go to www.oracle.com.

3. When the script responds with the **Trust this certificate?** prompt, type **Yes** and press **Enter**.
4. At the prompt for the keystore password, type in the following password and press **Enter**: `^8Bradford%23`
5. To view the certificate, navigate to the `/home/admin` directory and type the following: `keytool -list -v -keystore /bsc/campusMgr/.keystore`
6. Type the password used to import the certificate and press **Enter**.



The keystore is cached on startup. Therefore, it is recommended that you restart FortiNAC after making any changes to the keystore.

Obtaining an SSL certificate from a CA

If you do not have a certificate, you must obtain a certificate from a CA.

To obtain a valid third party SSL certificate from a CA, you must generate a CSR and send it to the CA.

1. Go to **System > Settings**.
2. Expand the **Security** folder.
3. Select **Certificate Management** from the tree.
4. Click **Generate CSR**.
5. Select the certificate target (the type of certificate you want to generate).
 - Select **Admin UI** to generate a CSR for the admin UI.
 - Select **Persistent Agent** to generate a CSR for the PA communications.
 - Select **Portal** to generate a CSR to secure the captive portal and DA communications.
 - Select **RADIUS Server** to generate a CSR for integrated FortiNAC RADIUS server set to use 802.1x and PEAP.
6. Enter the **Common Name**. This is the hostname to be secured by the certificate. If generating a wildcard CSR, enter the desired domain specifying the wildcard in the **Common Name** field (Example: *.example.com).
7. Enter the Subject Alternative Names (leave blank if not requesting a SAN certificate). Click **Add** to enter each additional hostname and/or IP address.
8. Enter the remaining information for the certificate in the dialog box:
 - **Organization**: The name of the server's organization.
 - **Organizational Unit**: The name of the server's unit (department).
 - **Locality (City)**: The city where the server is located.
 - **State/Province**: The state/province where the server is located.
 - **2 Letter Country Code**: The country code where the server is located.
9. Click **OK** to generate the CSR.
10. Copy the section with the certificate request to include the following:

```
-----BEGIN CERTIFICATE REQUEST-----  
...Certificate Request Data...  
-----END CERTIFICATE REQUEST-----
```
11. Paste it into a text file, and save the file with a .txt extension. Note the location of this file on your PC.
Make sure there are no spaces, characters, or carriage returns added to the certificate.
12. Send the certificate file to the CA to request a valid SSL certificate.

Important Notes:

- Do not click OK in the Generate CSR screen after saving the certificate file and sending to the CA. Each time OK is clicked on the Generate CSR screen, a new CSR and private key are created, overwriting any previous private key. Consequently, if a certificate file has been submitted to the CA, and **OK** has been clicked since the original certificate was generated, the returned certificate will not match the current private key, and a new request will have to be issued and sent to the CA.
- Not all certificate Authorities ask for the same information when requesting a certificate. For example, some CA's ask for a server type (Apache, etc) while others do not. FortiNAC requires a non-encrypted certificate in one of the following formats:
 - PEM
 - DER
 - PKCS#7
 - P7B

This will allow the certificate to be applied to any of the desired components.

If the certificate is in PEM format, opening the certificate in a text editor should look something like the following format:

```
-----BEGIN CERTIFICATE1-----
fjkghwjernlsfuigylerkjlkfjnu23jnlkjblu5ghl6kh4
fjkjlkfjnu23jnlkjblu5ghl6khkghwjernlsfuigyler4
ghwjernlsfuigylerkjlkfjnu23jnlkjblu5fjkghl6kh4
-----END CERTIFICATE1-----
-----BEGIN CERTIFICATE2-----
fjkghwjernlsfuigylerkjlkfjnu23jnlkjblu5ghl6kh4
fjkjlkfjnu23jnlkjblu5ghl6khkghwjernlsfuigyler4
ghwjernlsfuigylerkjlkfjnu23jnlkjblu5fjkghl6kh4
-----END CERTIFICATE2-----
```

Certificate requests generated on FortiNAC use the SHA1 RSA encryption signature. However, certificates with SHA2 encryption can be requested using this CSR.

Upload a certificate received from the CA

Upload the valid SSL certificate to the appliance when the certificate file is returned from the CA. Certificate files can be returned to you in one of several configurations. Depending upon the CA, one or multiple certificate files may be returned.

1. Save the file(s) received from the CA to your PC.
2. Select **System > Settings**.
3. Expand the **Security** folder.
4. Select **Certificate Management** from the tree.
5. Click **Upload Certificate**.
6. Select the target where the certificate will be uploaded:
 - Select **Admin UI** to install the certificate for the admin UI.
 - Select **Persistent Agent** to install certificate for the PA communications.
 - Select **Portal** to install the certificate to secure the captive portal.
7. Select one of the following:
 - **Use Private Key from Last Generated CSR** to use the key from the most recent CSR for the selected target.
 - **Reuse Private Key from Existing Certificate** to use the private key for the certificate currently in use. This option is for renewing an existing installed certificate.
 - **Upload Private Key** to upload a key. Click **Choose** to find and upload the private key.
8. Click **Choose File** to find and select the certificate to be uploaded. Users can also upload CA certificates and CA bundles.



Upload any relevant intermediate certificate files needed for the creation of a completed certificate chain of authority. The certificate Authority should be able to provide these files. Without a complete certificate chain of authority, the target functionality may produce error/warning messages.

9. Click **Add Certificate** if multiple certificates were returned. Use this to enter each additional certificate file.
10. Click **OK**.

Copying a certificate to another target

If the certificate is intended to be used for multiple targets, copy the certificate to the new target:

1. Highlight the target with the desired certificate installed.
2. Click **Copy Certificate**.
3. Select the new target from the drop-down menu.
4. Click **OK**.

Activating certificates

Certificates for the admin UI and Persistent Agent are activated automatically upon installation. No further action is required.

1. Navigate to **System > Settings**.
2. Expand the **Security** fold and then click **Portal SSL**.
3. In the **SSL Mode** field, select **Valid SSL Certificate**.
4. Click **Save Settings** (this may take several minutes).

Create expiration warning alarms

Three events are enabled by default in FortiNAC:

- **Certificate Expiration Warning**: Generated when a certificate is due to expire within 30 days.
- **Certificate Expiration Warning (CRITICAL)**: Generated when a certificate is due to expire within 7 days.
- **Certificate Expired**: Generated when a certificate has expired.

You must create alarms to send emails when these events are generated.

1. Navigate to **Logs > Events & Alarms > Mappings**.
2. Create one alarm for each event with the following settings:
 - Select the **Notify Users** setting.
 - Select the type of messaging (Email or SMS) and admin group desired to be notified.
 - Set the **Trigger Rule** to **One Event to One Alarm**.
3. For detailed instructions on creating alarms, see [Add or modify alarm mapping on page 787](#).

Renew a certificate

SSL certificates must be renewed periodically or they expire. However, the existing certificate must be used until the new one arrives. Some certificate Authorities allow managing certificates such that it can be renewed without generating a new request file. In these cases, the private key will remain the same and the new certificate can be imported when it arrives.

1. Save the file(s) received from the CA to your PC.
2. Select the target where the certificate will be uploaded. See Step 6 under [Upload a certificate received from the CA on page 512](#).
3. Select **Reuse Private Key from Existing Certificate** to use the private key for the certificate currently in use.

See Step 7 under [Upload a certificate received from the CA on page 512](#).

4. Follow Steps 8-10 under [Upload a certificate received from the CA on page 512](#) to complete the process.

Troubleshooting

If something is wrong with the uploaded certificate files, FortiNAC will display an error and will not apply the certificate.

Common causes for upload errors

- The wildcard name (e.g., *.example.com) was placed in the **Fully Qualified Host Name** field in the **Portal SSL** view under **System > Settings > Security**. To correct, change the entry to the true fully qualified hostname and click **Save Settings**.
- There are extra spaces, characters, and/or carriage returns above, below, or within the text body of any of the files.
- The certificate was not generated with the current key and there is mismatch.

This can happen if **OK** in the **Generate CSR** screen had been clicked after saving the certificate request. Each time **OK** is clicked on the **Generate CSR** screen, a new CSR and private key are created, overwriting any previous private key.

To confirm the certificate and key match, use the following tool:

<https://www.sslshopper.com/certificate-key-matcher.html>

If the key and certificate do not match, generate a new CSR and submit for a new certificate.

- An error displays indicating the private key is invalid. This can occur if the private key is not a RSA private key. To confirm, (if the certificate is in PEM format), open the certificate in a text editor. If the content looks something like the following:

```
-----BEGIN PRIVATE KEY-----
MIIEowIBAAKCAQEAtozSKRv4mpPVk0L4Xz2RzadYym5pRH+Cp1du4uJ2yGKepFmF
HoB/yOuBt0PAJz9SAT+CkK7j5ocWbAlkjtZxdSs5T2aABWIWTmu015T8GYD6KQ9T
-----END PRIVATE KEY-----
```

then the key will need to be converted to a RSA key.

- The following error displays in UI: "Unable to update Apache configuration." This can occur if SSH communication is failing (as the appliance establishes a SSH session to restart apache service). Verify appliance can SSH to itself (without being prompted to enter a password).



For additional troubleshooting assistance, contact [Fortinet Support](#).

DNS server configuration

FortiNAC has its own DNS server used to manage page resolution in the captive portal. This DNS server contains specific SRV records used by the FortiNAC agent technology to locate the server while in isolation. These records indicate the port and FQDN of the FortiNAC appliance where the portal is located.

The Configuration Wizard adds the SRV records to the domain.zone.* files for the named service during the initial appliance configuration. Files are created and updated based upon the isolation interfaces configured (e.g. Isolation, Registration, Remediation, etc). Manual edits to these files are not needed and should not be attempted.

If you use agents for macOS and some Linux systems, using a .local suffix in **Domain** fields in the Configuration Wizard may cause communications issues.

Example:

Incorrect DNS suffix for reg: `tech-reg.megatech.local`

Correct DNS suffix for reg: `tech.megatech-reg.edu`

If you are unable to configure the agent through Agent Configuration, the same SRV records may be added to the corporate production DNS servers. These are particularly important in a high availability environment because the SRV records provide the agent with a prioritized list of servers with which it can communicate. In a facility where multiple FortiNAC appliances are being managed by a FortiNAC Manager, SRV records make it easier for the agent to locate a FortiNAC server.

When using the FortiNAC Manager to manage multiple FortiNAC servers, enabling the **Require Connected Adapter** check box in Persistent Agent Properties eliminates the need to use ACLs to block access to the FortiNAC server when the host is connecting on a device managed by a different FortiNAC Server. This setting will require a host reported by the agent to be connected to a device managed by FortiNAC in order to communicate.

To enable the **Require Connected Adapter** check box, go to **System > Settings > Passive Agent > Properties**.

The agent must be configured with security enabled.

When **Require Connected Adapter** is disabled, you must use ACLs to block access to a FortiNAC server when the host is connecting on a device managed by a different FortiNAC Server. For example, assume the host initially connects to the network on Device A which is managed by Server A. When the host later connects to the network on Device B which is managed by Server B, the agent continues to communicate with Server A. If access to Server A is denied, the agent will go through the server discovery process to locate another server.

Entries in DNS are different for each agent. Currently, the DNS mechanism used for the agent to discover the server is used by the Mobile Agent, Dissolvable Agent, and Persistent Agent. As new types of agents are added to FortiNAC you may be required to update DNS SRV records to accommodate them. See [Agent server discovery on page 519](#).

Verify the SRV records

1. Log into the CLI of the FortiNAC appliance that is running the captive portal, typically this is a FortiNAC Application Server.
2. Navigate to the following directory: `/var/named/chroot/etc`
3. There is a special zone file for the Mobile Agent labeled `discovery.portal.bradfordnetworks.com.zone`. Type `ls *.zone` and verify that this file is in the list of files.
4. Type `ls domain.zone.*` to display a list of all of the domain.zone files.
5. Display the contents of one of the files by typing `cat <file name>`, for example, `cat domain.zone.reg.`
6. Within the contents displayed look for the lines beginning with `_bradfordagent.`

If those lines are included in the file, then the SRV records have been added to the domain.zone.* files. You should see records similar to the following:

```
$TTL 15s
example.com.      IN SOA reg.example.com. root.reg.example.com. (
                  1
                  10800
                  3600
                  604800
```

```

                                86400
                                )
                                IN NS      reg.example.com.
                                IN TXT      "Registration Domain"
$ORIGIN example.com.

b._dns-sd._udp PTR @
lb._dns-sd._udp PTR @
_networksentry._tcp PTR AgentConfig._networksentry._tcp

;Insert agent line here
; Needs to be here for BN_OTHER_HOSTNAME
AgentConfig._networksentry._tcp SRV 0 0 443 servername.domainname.com.
                                TXT path=/registration/agent/config
_networksentry._tcp             SRV 0 0 443 servername.domainname.com.
                                TXT path=/registration/agent/config

_bradfordagent._tcp             SRV 0 0 4568 servername.domainname.com.
*.example.com.                  IN      A      172.16.28.1

```

Adding a DNS SRV record

DNS servers will vary based on the operating system of the computer used to house them. The example below is for a DNS server running on a Windows operating system with the SRV records added from a command prompt. You may prefer to use another method to add records to your DNS Server.

1. On the Windows Desktop click **Start > Run**.
2. On the **Run** dialog in the **Open** field, type `command` and click **OK**.
3. At the command prompt type the following:

```
> dnscmd /RecordAdd yourdomain.com _bradfordagent._tcp.yourdomain.com. SRV 0 0 4568
servername.domainname.com.
```

In the commands above `yourdomain.com` is the zone supplied via DHCP (Connection-specific DNS Suffix on a Windows station in "ipconfig /all" output). `servername.domainname.com` is the FQDN of the FortiNAC Application Server or server that is running the captive portal. Note that there is a period (.) after `.com` at the end of the FQDNs and node names.

The two zeros (0) in the example indicate priority and weight of this record. Priority is used when there are multiple servers to which the agent can connect, such as in a high availability environment.

DNS server examples

From the DNS example in the section above you must include specific entries in your production DNS server. The examples below list each entry and provide notes about its function and the agents affected.

Entry 1

This entry is used only by the Dissolvable Agent. It is always required.

```
_networksentry._tcp PTR AgentConfig._networksentry._tcp
```

```
AgentConfig._networksentry._tcp SRV 0 0 443 servername.domainname.com.  
                                TXT path=/registration/agent/config  
_networksentry._tcp SRV 0 0 443 servername.domainname.com.  
                                TXT path=/registration/agent/config
```

Entry 1 example using Windows command prompt

```
nslookup /RecordAdd domainname.com _networksentry._tcp PTR AgentConfig._networksentry._tcp.
```

```
nslookup /RecordAdd domainname.com AgentConfig._networksentry._tcp SRV 0 0 443  
servername.domainname.com.
```

```
nslookup /RecordAdd domainname.com AgentConfig._networksentry._tcp TXT  
path=/registration/agent/config
```

```
nslookup /RecordAdd domainname.com _networksentry._tcp SRV 0 0 443 servername.domainname.com.  
nslookup /RecordAdd domainname.com _networksentry._tcp TXT path=/registration/agent/config
```

These lines work together to define the AgentConfig service. The first line indicates the name of the service and sets the type (`_networksentry._tcp`).

The second and third lines are the SRV record and indicate the FQDN of the server to which the agent will connect. The two zeros (0) in the example indicate priority and weight of this record. Priority is used when there are multiple servers to which the agent can connect, such as in a high availability environment. 443 is the port and should not be changed. In the example, the name of the server is `servername.domainname.com`. This must match the name in the valid certificate used to secure the portal. Note that the period (.) at the end of `servername.domainname.com` is required. The TXT line contains the path.

The agent uses the information contained in these entries to construct a URL for the server to which it should connect. Using the records shown above the agent would construct the following:

```
https://servername.domainname.com:443/registration/agent/config
```

Entry 2

This entry is used by the Mobile Agent and is always required.

```
_networksentry._tcp.discovery.portal.bradfordnetworks.com SRV 0 0 443  
servername.domainname.com.
```

```
_networksentry._tcp.discovery.portal.bradfordnetworks.com TXT  
path=/registration/agent/config
```

These lines are SRV record and indicate the FQDN of the server to which the agent will connect. They are the detailed version of the lines below that are included in the `domain.zone.reg` file shown above. It is recommended that you use the detailed entry when editing your production DNS; however, either entry is acceptable.

```
_networksentry._tcp SRV 0 0 443 servername.domainname.com.  
TXT path=/registration/agent/config
```

The two zeros (0) in the examples indicate priority and weight of this record. Priority is used when there are multiple servers to which the agent can connect, such as in a high availability environment. 443 is the port and should not be

changed. In the example, the name of the server is `servername.domainname.com`. This must match the name in the valid certificate used to secure the portal. Note that the period (.) at the end of `servername.domainname.com` is required. The TXT line contains the path.

The agent uses the information contained in these entries to construct a URL for the server to which it should connect. Using the records shown above the agent would construct the following:

```
https://servername.domainname.com:443/registration/agent/config
```

Entry 3

This entry must be done on each site that uses the Persistent Agent.

```
_bradfordagent._tcp SRV 0 0 4568 servername.domainname.com.
```

These SRV records indicate the FQDN of the server to which the agent will connect. The two zeros (0) in the example indicate priority and weight of this record. Priority is used when there are multiple servers to which the agent can connect, such as in a high availability environment. 4568 is the port on which the server listens and should not be changed. In the example, the name of the server is `servername.domainname`. Note that the period (.) at the end of `servername.domainname.com` is required.

This entry is used by the Persistent Agent and is required. The Persistent Agent has other mechanisms for determining where its server is such as registry entries on the host or information contained in Persistent Agent Properties on the server. However, if those options are not available, the Persistent Agent does use DNS to locate a server.

See [Agent server discovery on page 519](#).

Entry 4

These records are used by the Persistent Agent.

In a high availability environment where redundant servers are not on the same sub-net and there is no shared IP address, you must add SRV records for all of the servers in order by priority. Priority is the first number after SRV in the example. If your high availability servers share an IP address you do not need to provide these entries. Use the entries for the stand-alone server as shown in the examples above for Entry 1 through Entry 4.

```
_bradfordagent._tcp.example.com SRV 0 0 4568 primaryas.example.com.  
_bradfordagent._tcp.example.com SRV 1 0 4568 secondaryas.example.com.
```

Entry 5

These records are used by the Persistent Agent.

In an environment where multiple FortiNAC servers are managed by a FortiNAC Manager, the best practice is to set the registry keys via software push. If this is not possible, there should be an entry in DNS for each FortiNAC appliance that runs a captive portal. If all servers are reachable across all segments of the network, you may need to create ACLs that block access for the Persistent Agent from one segment to another. When a host with the Persistent Agent installed moves from one location to another on the network the Persistent Agent will continue to connect to its original FortiNAC server. The agent will not connect to the server that is managing the port to which it is connected. If an ACL denies the Persistent Agent access to a FortiNAC server based on the hosts location on the network, the Persistent Agent will search for a different server.

The following shows DNS configuration entries for two FortiNAC configurations.

```
_bradfordagent._tcp.example.com SRV 0 0 4568 appserver1.example.com.  
_bradfordagent._tcp.example.com SRV 0 0 4568 appserver2.example.com.
```

In the commands above `example.com` is the zone. `appserver1.example.com` and `appserver2.example.com` are the FQDNs of the FortiNAC Application Servers or servers that are running the captive portal. Note that there is a period (.) after `.com` at the end of the FQDNs and node names.

Agent server discovery

Agent server discovery is a mechanism used by different types of agents to determine the identity of the FortiNAC Server or Application Server to which the agent should connect. Some agents use SRV and TXT records contained within both FortiNAC's DNS server (for when agents are in isolation) and your production DNS server. The records used by the Agent for identifying and connecting to the FortiNAC server vary depending on the type of Agent used.

FortiNAC agents discover the FortiNAC Application Server to which they should connect in variety of ways. The discovery process for each agent is outlined in this section.



The FortiNAC Application Server name used by the agent must match the server name in the certificate securing the appropriate certificate Target or the agent and the server will not be able to communicate. The certificate Target used is dependent upon the agent type. Refer to the discovery process below.

Persistent Agent

Persistent Agent v3.0 and higher determines the FortiNAC Application Server to which it should connect in several ways. If you have used the Administrative Templates distributed with FortiNAC and used Group Policy Objects to set registry entries on each host, then the Persistent Agent can use those entries to find the appropriate FortiNAC Application Server.

The Persistent Agent communicates on the following ports:

- tcp 4568
- tcp 80 (required for upgrades)

The discovery process is as follows:

1. The Persistent Agent starts.
2. The agent checks DNS for SRV records of `_bradfordagent._udp.example.com` and `_bradfordagent._tcp.example.com`.
3. The agent looks at the host registry (Windows), preferences (macOS), or `.conf` (Linux).
4. First it checks the entry for `lastConnectedServer`. If `lastConnectedServer` is set it adds the server to the top of the list.
5. Then it checks the entry for `HomeServer`. If `HomeServer` is set, it adds it to a list.
6. Then the agent checks the entry for `AllowedServers`. This entry contains a list of additional servers to which the agent can connect. It adds each of these servers to the list.
7. If SRV records are returned, the agent processes them in reverse priority order (highest value first). If `homeServer` is not already set, the name contained in the SRV response is written to the host registry `HKLM\Software\Bradford Networks\Client Security Agent` (Windows) or preferences (macOS, Linux).*
8. For each SRV record:
 - a. If the name is not already in the list, and `restrictRoaming` is disabled, the agent adds the name to the top of the list and to the `lastConnectedServer` value.
 - b. Otherwise, if the name is already in the list, the agent moves the name to the top of the list.

9. Now that the list of servers is complete, the agent tries to connect to each server over SSL/TLS until it successfully connects to one. Unless security is disabled on the agent, this is done over SSL/TLS (requires valid certificate installed for the Persistent Agent certificate Target).
10. Once the agent has successfully connected to a server, that server will be set to the lastConnectedServer value, and moved to the top of the list.
11. Once a server has been added to the lastConnectedServer, if restrictRoaming is enabled, it will remain at the top of the list until that server is no longer reachable by the agent. At that point the list will be parsed until the agent connects to a server and then that server will be moved to lastConnectedServer and to the top of the list.

*registry/preferences settings remain until one of the following occurs:

- Entry is manually changed.
- Agent is uninstalled.
- Agent is updated.

If the agent cannot be configured through Agent Configuration, the same SRV records may be added to the corporate production DNS servers. Agents can then query the DNS servers to determine the FortiNAC server with which they should communicate.

Mobile Agent

The Mobile Agent determines the FortiNAC Application Server to which it should connect by checking DNS as follows:

1. The Mobile Agent starts.
2. It checks DNS and is directed to a service type _networksentry.tcp called AgentConfig.
3. It checks the SRV record for that service type for the server to which it should connect.
4. It connects to the FortiNAC Application Server over SSL/TLS (requires valid certificate installed for the Portal certificate Target).
5. For Mobile Agent 3.1 or higher, if for any reason it cannot connect to the FortiNAC Application Server, a request for the appropriate URL is presented to the user. The URL field will accept an HTTPS address, the FQDN of the server which it uses to create an HTTPS address or an HTTP address. If an HTTP address is used, a warning is displayed asking the user to confirm that they wish to access the server over an insecure connection.

Passive Agent

The Passive Agent determines the FortiNAC Application Server to which it should connect by checking the host registry.

1. The network user logs onto the network.
2. The login triggers a script that is served from a corporate server on the network.
3. The script checks the registry entry ServerURL for the list of servers to which it can connect.
4. It tries the servers in order until it connects to one.

Dissolvable Agent

The Dissolvable Agent determines the FortiNAC Application Server to which it should connect by checking DNS as follows:

1. The Dissolvable Agent starts.
2. It checks DNS and is directed to a service type _networksentry.tcp called AgentConfig.
3. It checks the SRV record for that service type for the server to which it should connect.
4. It connects to the FortiNAC Application Server over SSL/TLS (requires valid certificate installed for the Portal certificate Target).

5. If for any reason it cannot connect to the FortiNAC Application Server, a request for the appropriate URL is presented to the user. The URL field will accept an HTTPS address, the FQDN of the server which it uses to create an HTTPS address or an HTTP address. If an HTTP address is used, a warning is displayed asking the user to confirm that they wish to access the server over an insecure connection.

Persistent Agent on Windows

To take advantage of the Agent Security feature some settings must be configured on the host. Settings for Windows hosts are configured in the registry. Settings for Mac OS X hosts are configured in Preferences.

Administrative templates are used to configure registry settings on Windows endpoints through Group policy objects. These templates can be downloaded from the Agent Distribution view in FortiNAC. Customers can opt to edit registry settings on hosts using another tool.

Requirements:

- Active Directory
- Group Policy Objects
- Template Files From

Templates:

The templates listed below are provided by Fortinet. You must run the installation program for the templates on your Windows server or another Windows system and then copy files to your server. Be sure to select the appropriate MSI for your architecture.

- 32-bit (x86): Bradford Networks Administrative Templates.msi
- 64-bit (x86_64): Bradford Networks Administrative Templates-x64.msi

Install ADMX template

1. In FortiNAC select **Policy > Agent Distribution**.
2. At the top of the Agent Distribution window click either the **32-bit (x86)** or the **64-bit (x86_64)** link to download the appropriate template file.
3. Copy the template file to the domain server or another Windows system with access to the Central Store or local PolicyDefinitions directory.
4. On the Windows system, double-click the msi file to start the installation wizard.
5. Click through the installation wizard.
6. Browse to `Program Files\Bradford Networks\Administrative Templates\admx`.
7. Copy the `Bradford Networks.admx` and `en-US` directory to the `PolicyDefinitions` directory of your central store.
8. Open the Group Policy Editor and navigate to the **Group Policy Object** you want to edit, right-click and select **Edit** to display the **GPO Editor** pane.
9. Browse to **Computer Configuration > Administrative Templates > Bradford Networks**.

Install GPO template

1. In FortiNAC select **Policy > Agent Distribution**.
2. At the top of the Agent Distribution window click either the **32-bit (x86)** or the **64-bit (x86_64)** link to download the appropriate template file.
3. Copy the template file to the domain server.
4. On the domain server, double-click the msi file to start the installation wizard.
5. Click through the installation wizard. At the end, the Microsoft Group Policy Management Console will be launched, if available.
6. Navigate to the **Group Policy Object** you want to edit, right-click and select **Edit** to display the GPO Editor pane.
7. Right-click **Computer Configuration > Administrative Templates** and select **Add/Remove Templates**, shows the current templates pop-up.
8. Click **Add** and browse to `Program Files\Bradford Networks\Administrative Templates`.
9. Select `Bradford Persistent Agent.adm` and click **Open**.
10. Click **Close**, and the administrative templates will be imported into the GPO.

Install an updated template

Occasionally new templates are made available to incorporate additional features. If you already have a Fortinet Administrative Template installed but it does not have Balloon Notifications enabled, follow the instructions below to update it. If you do have Balloon Notifications enabled, see [Agent packages on page 992](#) for instructions on installing an updated template.

1. On your Windows server open the Group Policy Management Tool.
2. Navigate to the **Group Policy Object** you want to edit, right-click and select **Edit** to display the GPO Editor pane.
3. Right-click **Computer Configuration > Administrative Templates** and select **Add/Remove Templates**, to show the current templates pop-up.
4. Select the old template and click **Remove**. Follow the instructions above to install the new template.

Persistent Agent settings

The table below outlines settings that can be configured for the Persistent Agent.

Setting	Options
Allowed Ciphers and Authentication Schemes	Indicates the cipher and authentication schemes that can be used.
CA Trust Length/ Depth	Indicates how deep a chain of certificates to allow between the server's certificate and the certificate's Central Authority.
CA File path	The absolute path to a file containing root and intermediate CA certificates in PEM format.
Security	Indicates whether security is enabled or disabled. Note: This option is no longer available with agent 5.3 and greater. Security is always enabled.

Setting	Options
Home Server	The fully qualified hostname of the default server with which the agent should communicate. If this server is not set, it is automatically discovered using Server Discovery. On upgrade, this is populated by the contents of ServerIP.
Allowed Servers	In large environments there may be more than one set of FortiNAC servers. If roaming between servers is limited, list the FQDNs of the FortiNAC Application Server or FortiNAC Servers with which the agent can communicate.
Restrict Roaming	If enabled, the agent communicates only with its Home Server and servers listed under Allowed Servers. If disabled, the agent searches for additional servers when the home server is unavailable.
maxConnectInterval	The maximum number of seconds between attempts to connect to FortiNAC. Data Type: Integer Default: 960
Last Connected Server	Server that the agent last connected to and with which the agent always attempts to communicate first. Protocol configuration change requests are honored only when they are received from this server. If this server is not set, it is automatically discovered using Server Discovery.
Discover Servers, Priority, and Ports	Enable or Disable the Agent Discovery Features. Requires Persistent Agent 5.3.0 or newer.



Refer to the **Registry Keys** section in [Administrative templates for GPO on page 608](#) for more information about the registry keys that correspond to the Persistent Agent settings.

Registry keys

The table below shows the host's registry keys that are not modified by the Group Policy Object. These keys can be set manually.

Key	Value	Data
Persistent Agent		
HKLM\Software\Bradford Networks\Client Security Agent For 64-bit operating systems see Note.	ServerIP	The fully qualified hostname to which the agent should communicate. Data Type: String Default: ns8200
HKLM\Software\Bradford Networks\Client Security Agent For 64-bit operating systems see Note.	ClientStateEnabled	0: Do not show balloon notifications on status changes. 1: Show balloon notifications on status changes. Data Type: DWORD

Key	Value	Data
		Default: 1
HKLM\Software\Bradford Networks\Client Security Agent	ShowIcon	0: Do not show the tray icon. 1: Show the tray icon. Data Type: DWORD Default: Not Configured (Tray icon displayed)
HKLM\Software\Bradford Networks\Client Security Agent For 64-bit operating systems see Note.	allowedServers	Comma-separated list of fully qualified hostnames with the agent can communicate. If restrict roaming is enabled, the agent is limited to this list. The home server does not need to be included in this list (for example, a.example.com, b.example.com, c.example.com). Data Type: String Default: Empty
HKLM\Software\Bradford Networks\Client Security Agent	homeServer	The fully qualified hostname of the default server with which the agent should communicate. Data Type: String Default: Empty
HKLM\Software\Bradford Networks\Client Security Agent	restrictRoaming	0: Do not restrict roaming. Allow agent to communicate with any server. 1: Restrict roaming to the home server and the allowed servers list. Data Type: Integer Default: 0
HKLM\Software\Bradford Networks\Client Security Agent	securityEnabled	0: Disable Agent Security. 1: Enable Agent Security Data Type: Integer Default: 1 Agent 5.3 and greater: Security is always enabled.
HKLM\Software\Bradford Networks\Client Security Agent	ServerIP	The fully qualified hostname to which the agent should communicate. Data Type: String Default: ns8200
HKLM\Software\Bradford Networks\Client Security Agent For 64-bit operating systems see Note.	maxConnectInterval	The maximum number of seconds between attempts to connect to FortiNAC. Data Type: Integer Default: 960

Key	Value	Data
HKLM\Software\Bradford Networks\Client Security Agent For 64-bit operating systems see Note.	lastConnectedServer	The last server that the Agent successfully connected to. This will be automatically populated by the agent upon successfully connection to a server discovered through SRV records, or from homeServer, or allowedServers list. This value will remain unchanged until the lastConnectedServer is unreachable by the agent and the agent has connected to another server. Data Type: String Default: Empty
HKLM\Software\Bradford Networks\Client Security Agent HKLM\Software\wow6432node	discoveryEnabled	Enable or Disable Discovery via SRV. The agent will search for SRV Records to prioritize servers and override default ports. If connections to servers are not limited, agents will connect to the discovered server names as well. 0: Disable Discovery. 1: Enable Discovery Data Type: Integer Default: 1



On 64-bit operating systems in RegEdit, these registry values will appear in the following key:
HKLM\Software\wow6432node



Disabling the tray icon via the registry requires the Persistent Agent.



Individual User keys are required only when the user's settings differ from those for a group of users. Typically, keys are set based on a group of users who have a common Policy using the HKLM\Software\Bradford Networks\Client Security Agent key shown in the table.

Persistent Agent on macOS

To take advantage of the Agent Security some settings must be configured on the host. Settings for Mac OS X hosts are configured in Preferences. At this time we do not have a recommendation for a tool to set preferences.

Security settings

The table below outlines settings that can be configured for Agent Security.

Setting	Options
Allowed Ciphers and Authentication Schemes	Indicates the cipher and authentication schemes that can be used.
CA Trust Length/ Depth	Indicates how deep a chain of certificates to allow between the server's certificate and the certificate's Central Authority.
CA File path	The absolute path to a file containing root and intermediate CA certificates in PEM format.
Security	Indicates whether security is enabled or disabled. Note: This option is no longer available with agent 5.3 and greater. Security is always enabled.
Home Server	The fully qualified hostname of the default server with which the agent should communicate. If this server is not set, it is automatically discovered using Server Discovery. On upgrade, this is populated by the contents of ServerIP.
Allowed Servers	In large environments there may be more than one set of FortiNAC servers. If roaming between servers is limited, list the FQDNs of the FortiNAC Application Server or FortiNAC Servers with which the agent can communicate.
Restrict Roaming	If enabled, the agent communicates only with its Home Server and servers listed under Allowed Servers. If disabled, the agent searches for additional servers when the home server is unavailable.
maxConnectInterval	The maximum number of seconds between attempts to connect to FortiNAC. Data Type: Integer Default: 960
Last Connected Server	Server that the agent last connected to and with which the agent always attempts to communicate first. Protocol configuration change requests are honored only when they are received from this server. If this server is not set, it is automatically discovered using Server Discovery.
Discover Servers, Priority, and Ports	Enable or Disable the Agent Discovery Features. Requires Persistent Agent 5.3.0 or newer.

Preferences

The table below shows the modifications that need to be made to the host's Preferences. If you use a tool other than GPO, you must make sure to set the appropriate keys on each host.

Value	Data
allowedServers	Comma-separated list of fully qualified hostnames with the agent can communicate. If restrict roaming is enabled, the agent is limited to this list. The home server does not need to be included in this list (for example, a.example.com, b.example.com, c.example.com). Agents 10.7 and above: Port can also be specified (<Fully qualified hostname>:<port>). The default port if not specified is 4568.

Value	Data
	Example: a.example.com:9001, b.example.com:4568, c.example.com:4985 Data Type: String Default: Empty
homeServer	The fully qualified hostname of the default server with which the agent should communicate. Example: a.example.com Agents 10.7 and above: Port can also be specified (<Fully qualified hostname>:<port>). The default port if not specified is 4568. Example: a.example.com:9001 Data Type: String Default: Empty
restrictRoaming	0: Do not restrict roaming. Allow agent to communicate with any server. 1: Restrict roaming to the home server and the allowed servers list. Data Type: Integer Default: 0
securityEnabled	0: Disable Agent Security. 1: Enable Agent Security Data Type: Integer Default: 1 Agent 5.3 and greater: Security is always enabled.
ServerIP	The fully qualified hostname to which the agent should communicate. Data Type: String Default: ns8200
ShowIcon	0: Do not show the tray icon. 1: Show the tray icon. Default: Not Configured (Tray icon displayed)  If both com.bradfordnetworks.bndaemon and com.bradfordnetworks.bndaemon.policy are configured on the system, the com.bradfordnetworks.bndaemon.policy configuration takes precedence over the com.bradfordnetworks.bndaemon configuration.
maxConnectInterval	The maximum number of seconds between attempts to connect to FortiNAC. Data Type: Integer Default: 960

Value	Data
lastConnectedServer	The last server that the Agent successfully connected to. This will be automatically populated by the agent upon successfully connection to a server discovered through SRV records, or from homeServer, or allowedServers list. This value will remain unchanged until the lastConnectedServer is unreachable by the agent and the agent has connected to another server. Data Type: String Default: Empty
discoveryEnabled	Enable or Disable Discovery via SRV. The agent will search for SRV Records to prioritize servers and override default ports. If connections to servers are not limited, agents will connect to the discovered server names as well. 0: Disable Discovery. 1: Enable Discovery Data Type: Integer Default: 1

There are manual commands that can be used to modify the Preferences as follows:

1. On the macOS host, navigate to a command prompt (Terminal).
2. Before editing the preferences, it is recommended that you unload the launchDaemon plist. Type the following:

```
sudo launchctl unload /Library/LaunchDaemons/com.bradfordnetworks.agent.plist
```
3. To read the configuration, type the following:

```
sudo defaults read /Library/Preferences/com.bradfordnetworks.bndaemon
```
4. To write configuration values use the table above for the value names and type a command similar to the following:

```
sudo defaults write /Library/Preferences/com.bradfordnetworks.bndaemon homeServer -string qa225.bradfordnetworks.com
```

In the example above, homeServer is the value name, -string is the data type, qa225.bradfordnetworks is the data or setting that should be added to Preferences.
5. While some elements require a string data value, others require an integer data value. For these elements, type a command similar to the following:

```
sudo defaults write /Library/Preferences/com.bradfordnetworks.bndaemon restrictRoaming -int 1
```

In the example above, restrictRoaming is the value name, -int is the value data type and 1 is the setting added to the value. In this case 1 is equal to enabled and 0 is disabled.
6. To reload the launchDaemon plist, type the following:

```
sudo launchctl load /Library/LaunchDaemons/com.bradfordnetworks.agent.plist
```

Persistent Agent on Linux

To take advantage of the Agent Security some settings must be configured on the host. Settings for Linux hosts are configured in the configuration file located at /etc/xdg/com.bradfordnetworks/PersistentAgent.conf

Security settings

The table below outlines settings that can be configured for Agent Security.

Setting	Options
Allowed Ciphers and Authentication Schemes	Indicates the cipher and authentication schemes that can be used.
CA Trust Length/ Depth	Indicates how deep a chain of certificates to allow between the server's certificate and the certificate's Central Authority.
CA File path	The absolute path to a file containing root and intermediate CA certificates in PEM format.
Security	Indicates whether security is enabled or disabled. Note: This option is no longer available with agent 5.3 and greater. Security is always enabled.
Home Server	The fully qualified hostname of the default server with which the agent should communicate. If this server is not set, it is automatically discovered using Server Discovery. On upgrade, this is populated by the contents of ServerIP.
Allowed Servers	In large environments there may be more than one set of FortiNAC servers. If roaming between servers is limited, list the FQDNs of the FortiNAC Application Server or FortiNAC Servers with which the agent can communicate.
Restrict Roaming	If enabled, the agent communicates only with its Home Server and servers listed under Allowed Servers. If disabled, the agent searches for additional servers when the home server is unavailable.
maxConnectInterval	The maximum number of seconds between attempts to connect to FortiNAC. Data Type: Integer Default: 960
Last Connected Server	Server that the agent last connected to and with which the agent always attempts to communicate first. Protocol configuration change requests are honored only when they are received from this server. If this server is not set, it is automatically discovered using Server Discovery.
Discover Servers, Priority, and Ports	Enable or Disable the Agent Discovery Features. Requires Persistent Agent 5.3.0 or newer.

Configuration settings

The table below shows the modifications that need to be made to the host's Preferences. If you use a tool other than GPO, you must make sure to set the appropriate keys on each host.

Value	Data
allowedServers	Comma-separated list of fully qualified hostnames with the agent can communicate. If restrict roaming is enabled, the agent is limited to this list. The home server does not need to be included in this list (for example, a.example.com, b.example.com, c.example.com). Data Type: String Default: Empty

Value	Data
homeServer	The fully qualified hostname of the default server with which the agent should communicate. Data Type: String Default: Empty
restrictRoaming	False: Do not restrict roaming. Allow agent to communicate with any server. True: Restrict roaming to the home server and the allowed servers list. Data Type: Boolean Default: False
securityEnabled	False: Disable Agent Security. True: Enable Agent Security Data Type: Boolean Default: True Agent 5.3 and greater: Security is always enabled.
ServerIP	The fully qualified hostname to which the agent should communicate. Data Type: String Default: ns8200
caFile	The absolute path to a file containing root and intermediate CA certificates in PEM format. Data type: String Default: /etc/ssl/certs/ca-bundle.crt (RPM) or /etc/ssl/certs/ca-certificates.crt (DEB)
ShowIcon	0: Do not show the tray icon. 1: Show the tray icon. Default: Not Configured (Tray icon displayed)  If both PersistentAgent.conf and PersistentAgentPolicy.conf are configured on the system, the PersistentAgentPolicy.conf configuration takes precedence over the PersistentAgent.conf configuration.
maxConnectInterval	The maximum number of seconds between attempts to connect to FortiNAC. Data Type: Integer Default: 960
macpollinterval	The maximum number of seconds between attempts to learn of new MAC address added to the host. This is intended to facilitate the quick discovery of VM Guests that have been deployed for use with the VM-Detection feature. Data Type: Integer Default: 5

Value	Data
lastConnectedServer	The last server that the Agent successfully connected to. This will be automatically populated by the agent upon successfully connection to a server discovered through SRV records, or from homeServer, or allowedServers list. This value will remain unchanged until the lastConnectedServer is unreachable by the agent and the agent has connected to another server. Data Type: String Default: Empty
discoveryEnabled	Enable or Disable Discovery via SRV. The agent will search for SRV Records to prioritize servers and override default ports. If connections to servers are not limited, agents will connect to the discovered server names as well. 0: Disable Discovery. 1: Enable Discovery Data Type: Integer Default: 1

Auto-definition updates

Updates are made available by Fortinet on a periodic basis for the following items:

- Vendor OUIs released by the IEEE Standards Association (see [Vendor OUIs](#)).
- Agent Templates which apply to the components available for evaluation during an Endpoint Compliance scan (for details see [Add or modify a scan](#)):
 - Endpoint operating system versions
 - Antivirus products and versions
 - Non-antivirus products (Miscellaneous)
 - Custom scan options

FortiNAC is configured, by default, to check for updates regularly using the **Auto-Definition Synchronization** task in [Scheduler](#). If updates are available for either the vendor OUIs or Agent template, they are downloaded and applied transparently.

The FortiNAC server retrieves the auto-definition updates from the Fortinet download site. Configure access to the site under **System > Settings > Updates > System Updates**.

Fortinet maintains the current update plus the previous three for administrators who prefer to download updates on a delayed schedule.

For details on configuring Fortinet download site access and auto-definition update schedule, see [System update](#).

Note: Auto-Definition updates are released independently of FortiNAC software and on a more frequent basis.

Policies

Endpoint compliance policies are used to assess hosts and determine if they are safe. An endpoint compliance policy is composed of building blocks, including: a user/host profile and an endpoint compliance configuration. Refer to

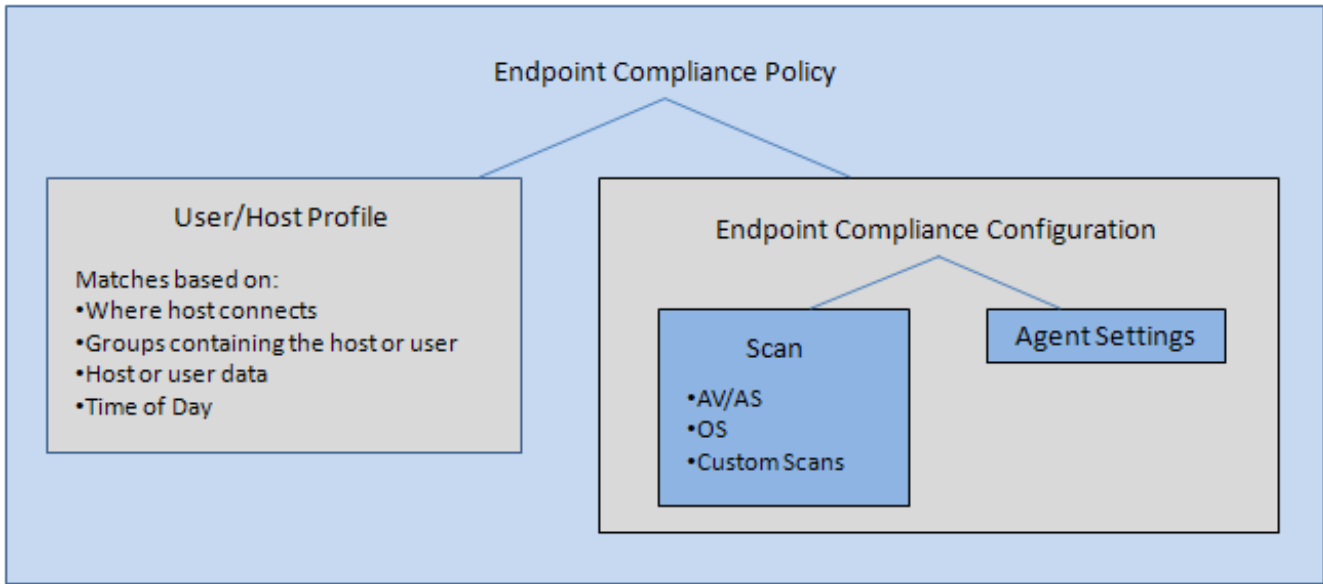
[Implementation on page 489](#) for information on the entire endpoint compliance feature.

When a host is evaluated and FortiNAC determines that the host requires an endpoint compliance policy, the host and user are compared to the user/host profiles within each endpoint compliance policy starting with the first policy in the list. When a match is found, the endpoint compliance policy is applied. Once a policy is selected as a match for the host or user, the endpoint compliance configuration within the policy determines the treatment that the host receives. An endpoint compliance configuration specifies whether or not an agent is required and the scan parameters for scanning the host.

Endpoint compliance policies created on the FortiNAC server will be ranked above global endpoint compliance policy created on the FortiNAC Manager. The rank of a local endpoint compliance policy can be adjusted above or below another local endpoint compliance policy, but cannot be ranked below a global endpoint compliance policy. The rank for a global endpoint compliance policy cannot be modified from the FortiNAC server.

If the user/host does not match any policy, it is allowed to register with no scan and no policy.

There may be more than one endpoint compliance policy that is a match for this host/user; however, the first match found is the one that is used.



If you create a user/host profile with fields Where set to Any, Who/What by Group set to Any, Who/What by Attribute set to Any and When set to Always, it matches ALL users and hosts. This is essentially a Catch All profile. If this user/host profile is used in a policy, all policies below that policy are ignored when assigning a policy to a user or a host. To highlight this, policies below the policy with the catch all profile are grayed out and have a line through the data.

The best way to use a Catch All profile is to create a general policy with that profile and place it last in the list of policies.

Settings

Field	Definition
Rank Buttons	Moves the selected policy up or down in the list. Host connections are compared to Policies in order by rank.

Field	Definition
Set Rank Button	Allows you to type a different rank number for a selected policy and immediately move the policy to that position. In an environment with a large number of policies, this process is faster than using the up and down Rank buttons.  Rank can only be set on local policies, rank changes for global policies must be done at the FortiNAC Manager.
Table columns	
Rank	Policy's rank in the list of policies. Rank controls the order in which host connections are compared to Policies.
Name	User defined name for the policy.
Endpoint Compliance Configuration	Contains the configuration for the Agent and Scan parameters that will be assigned if this Policy matches the connecting host and user. See Configurations on page 536 .
User/Host Profile	Contains the required criteria for a host or user, such as connection location, host or user group membership, host or user attributes or time of day. Host connections that match the criteria within the user/host profile are assigned the associated endpoint compliance configuration. See User/host profiles on page 466 .
Where	The connection location specified in the user/host profile. The host must connect to the network on a device, port or SSID contained within one of the groups shown here to be a match. When set to Any, this field is a match for all hosts or users.
Who/What	Attributes A host or user must meet all parameters within a single filter, but is only required to match one filter in the list. The attribute must be known at the time of connection. See Filter example on page 468. Note: Adapter status (Adapter -> Connected -> Online/Offline) should not be used for Network Access Policies. Adapter status changes as part of the authentication process and at the time of RADIUS authentication (FNAC post-auth processing), the adapter status will always be offline. RADIUS Attributes Used to match against endpoints pre- and post-authentication. Groups - Any — Matches any group. - Any Of — Matches any of the listed groups. Does not have to match everything, but has to match at least one group that has been selected. - All Of — Has to match every group that's been selected. - None Of — Has to match no group that's been selected.
When	The time frame specified in the selected User/Host Profile. The host must be on the network within this time frame to be a match. When set to Always this field is a match for all hosts or users.

Field	Definition
Note	User specified note field. This field may contain notes regarding the data conversion from a previous version of FortiNAC.
Last Modified By	User name of the last user to modify the policy.
Last Modified Date	Date and time of the last modification to this policy.
Right click options	
Delete	Deletes the selected endpoint compliance policy.
Modify	Opens the Modify Endpoint Compliance Policy window for the selected policy.
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746 .
 You must have permission to view the admin auditing log. See Add an administrator profile on page 139.	

Add or modify a policy

1. Select **Policy & Objects**.
2. Select **Endpoint Compliance**.
3. Click **Add** or select an existing policy and click **Modify**.
4. Click in the **Name** field and enter a name for this policy.
5. Select a **User/Host Profile** from the drop-down menu. You can use the icons next to the User/Host Profile field to add a new profile or modify the profile shown in the drop-down menu. Note that if you modify this profile, it is modified for all features that make use of the profile. Connecting hosts must match this User/Host Profile to be assigned the endpoint compliance configuration specified in the next step.
6. Select an **Endpoint Compliance Configuration** from the drop-down menu. You can use the icons next to the **Endpoint Compliance Configuration** field to add a new configuration or modify the configuration shown in the drop-down menu. Note that if you modify this configuration, it is modified for all features that make use of it. See [Create or edit a configuration on page 537](#).
7. The **Note** field is optional.
8. Click **OK** to save your policy.

Determining host operating system

FortiNAC uses the information configured in the endpoint compliance policy and information received from the connecting host to determine if an agent is required and which agent should be offered to a host. If the operating system or host type is one for which there is no agent, FortiNAC can allow or deny network access based on the settings in the endpoint compliance policy.

The host operating system is detected based on the information contained in the UserAgent string. When a host connects to a FortiNAC web page, its browser sends the user-agent string to the FortiNAC Server or Application Server.

This string indicates which browser the host is using, its version number, and details about the host, such as operating system and version. The chart below outlines the criteria FortiNAC uses to determine the host operating system.

Operating system is considered unsupported unless it meets one of the following criteria:

Criteria	OS/Device
UserAgent contains "linux" and "android"	Android
User Agent contains "linux" only	Linux
User Agent contains "macOS"	macOS
User Agent contains "Macintosh" and "Silk"	Android
User Agent contains "Macintosh" and "Cloud9"	Android
User Agent contains "linux", "android" and "silk"	Kindle
User Agent contains any one of the following: "KFOT", "KFTT", "KFJWI", "KFJWA", "KFSOWI", "KFTHWI", "KFTHWA", "KFAPWI" or "KFAPWA"	Kindle Fire
User Agent contains "macOS" and "mobile" and "ipod"	iOS for iPod
User Agent contains "macOS" and "mobile" and "iphone"	iOS for iPhone
User Agent contains "macOS" and "mobile" and "ipad"	iOS for iPad
User Agent contains "macOS" and "mobile"	Apple iOS
UserAgent contains "windows nt"	Windows
UserAgent contains "windows phone"	Windows Phone
UserAgent contains "windows nt" and "ARM"	Windows RT
UserAgent contains "freebsd"	Free BSD
UserAgent contains "openbsd"	Open BSD
UserAgent contains "netbsd"	Net BSD
UserAgent contains "solaris" or "sunos"	Solaris
UserAgent contains "symbianos" or "symbos"	Symbian
UserAgent contains "webos"	Web OS
UserAgent contains "windows ce"	Windows CE
UserAgent contains "blackberry"	Blackberry OS
UserAgent contains "BB10" and "Mobile"	BlackBerry 10 OS
UserAgent contains "RIM Tablet OS"	RIM Tablet OS
UserAgent contains "CrOS"	Chrome OS

Create or edit a policy

1. Select **Policy & Objects**.
2. Select **Endpoint Compliance**.
3. Click **Create New** or select an existing policy and click **Edit**.
4. Click in the **Name** field and enter a name for this policy.
5. Select a **User/Host Profile** from the drop-down menu. You can use the icons next to the **User/Host Profile** field to add a new profile or modify the profile shown in the drop-down menu. Note that if you modify this profile, it is modified for all features that make use of the profile. Connecting hosts must match this user/host profile to be assigned the endpoint compliance configuration specified in the next step.
6. Select an **Endpoint Compliance Configuration** from the drop-down menu. You can use the icons next to the **Endpoint Compliance Configuration** field to add a new configuration or modify the configuration shown in the drop-down menu. Note that if you modify this configuration, it is modified for all features that make use of it. See [Create or edit a configuration on page 537](#).
7. The **Note** field is optional.
8. Click **OK** to save your policy.

Delete a policy

1. Click **Policy & Objects**.
2. Select **Endpoint Compliance**.
3. Select the policy to be removed.
4. Click **Delete**.
5. Click **OK** to confirm that you wish to remove the policy.

Configurations

Endpoint compliance configurations define agent and scan parameters for hosts and users. Hosts can be required to download an agent and undergo a scan, permitted access with no scan or denied access. The endpoint compliance configuration that is used for a particular host is determined by the pairing of an endpoint compliance configuration and a user/host profile within an endpoint compliance policy.

When a host is evaluated, the host, user and connection location are compared to each endpoint compliance policy starting with the first policy in the list. When a policy is found where the host and user data and the connection location match the user/host profile in the policy, that policy is assigned. The endpoint compliance configuration contained within that policy determines the security treatment received by the host.

Settings

An empty field in a column indicates that the option has not been set.

Field	Definition
Name	User defined name for the Configuration.

Field	Definition
Scan	Name of the scan used to evaluate a connecting host.
Note	User specified note field. This field may contain notes regarding the conversion from a previous version of FortiNAC.
Collect Applications	If enabled, the agent assigned to the host will collect information about installed applications and add that information to the host record. An application inventory cannot be generated for a hosts unless an agent is in use.
Last Modified By	User name of the last user to modify the record.
Last Modified Date	Date and time of the last modification to this configuration.
Agent - OS	An Agent column is displayed for each operating system supported. The column contains the agent that will be used or treatment that applies to hosts with that operating system when the scan is applied. Some operating systems do not have agents and those hosts can only be allowed or denied access to the network. See Create or edit a configuration on page 537 for information on the agent options for each operating system.
Right click options	
Delete	Deletes the selected endpoint compliance configuration.
In Use	Indicates whether or not the selected configuration is currently being used by any other FortiNAC element. See Configurations in use on page 540 .
Modify	Opens the Modify Endpoint Configuration window for the selected configuration.
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746
 You must have permission to view the admin auditing log. See Add an administrator profile on page 139.	

Create or edit a configuration

1. Select **Policy & Objects**.
2. Expand **Endpoint Compliance**.
3. From the menu, select **Configuration**.
4. On the **Endpoint Compliance Configurations** window, click **Create New** or select an existing configuration and click **Edit**.
5. On the **General** tab, click in the **Name** field and enter a name for this configuration.
6. Select a **Scan** from the drop-down menu. You can use the icons next to the Scan field to add a new scan or modify the scan shown in the drop-down menu. Note that if you modify this scan, it is modified for all features that make use of it. See [Add or modify a scan on page 547](#).
7. If you would like to add a list of installed applications to the host record, enable the **Collect Application Inventory** check box. This only applies to hosts that are assigned an agent. An application inventory cannot be generated for hosts unless an agent is in use.

8. If you would like to add a whitelist of SSIDs that the endpoints can connect to, enable **Restrict Wireless Connections to Specific SSIDs**.
9. If you would like the endpoint compliance scans to check for Dual Homes connections, enable **Detect Multihoming**.
10. If you would like to grant varying levels of access based on the host's role, select **Advanced Scan Controls**. This displays additional options that allow you to select and map a security action to scan success, failure, and warning. See [Chaining configuration scans on page 540](#).
You must have Security Incidents access enabled to use the Advanced Scan Controls feature.
11. The **Note** field is optional.
12. Click the **Agent** tab to select it.
13. Select an agent for each operating system. You may choose not to use an agent for a particular operating system; however, scans can only be applied via an agent.
14. No agent exists for some operating systems. In those cases select either **None-Deny Access** or **None-Bypass**. Refer to the table below for information on each field.
15. Click **OK** to save the configuration.

Settings

Field	Definition
General tab	
Name	User specified name for this configuration.
Scan	Select the scan to be associated with this configuration. Hosts that match the endpoint compliance policy containing this configuration will be scanned with the selected Scan.
Collect Application Inventory	If enabled, the agent assigned to the host will collect information about installed applications and add that information to the host record. An application inventory cannot be generated for a hosts unless an agent is in use.
Advanced Scan Controls	If enabled, allows you to select a security action mapped to an endpoint compliance activity that will be taken based on scan results. See Chaining configuration scans on page 540 .
Note	User specified note field. This field may contain notes regarding the conversion of policies from a previous version of FortiNAC.
Agent tab	
Windows macOS Linux	Allows you to select a separate agent or treatment for each operating system. For example, a host with a Windows operating system may be scanned by the Persistent Agent while a host with a Mac operating system may be scanned with the Dissolvable Agent. See Determining host operating system on page 534. The names of all the agent versions and types available on the appliance are included in the list. The .exe is recommended for user-interactive installation. The .msi is recommended for use for a managed install by a non-user-interactive means. Agent options include: • Persistent Agent: Hosts with this operating system are required to download and install the selected version of the Persistent Agent. • Dissolvable Agent: Hosts with this operating system are required to download

Field	Definition
	and run the selected version of the Dissolvable Agent. • Persistent Agent: Hosts with this operating system are required to download and install the highest version of the Persistent Agent available on the FortiNAC Application server. Using the Latest Persistent Agent option prevents you from having to update Policies each time a new Agent is released and loaded onto your server. • None-Deny Access: No agent is assigned and hosts are denied access to the network if they have the matching operating system. • None-Bypass: No agent is assigned but hosts are allowed to access the network. If you select None - Bypass, hosts can register only if their IP address has been determined by FortiNAC. If IP address information has not been determined FortiNAC cannot determine the physical address and will not allow that host on the network. Users see the following message: Registration Failed - Physical Address not Found.
Android	• None-Deny Access: No agent is assigned and hosts are denied access to the network if they have the matching operating system. • None-Bypass: No agent is assigned but hosts are allowed to access the network if they have the matching operating system. • Mobile Agent: Mobile devices detected running the Android operating system are required to download and install the Mobile Agent. These devices are automatically directed to the Mobile Agent Download page in the captive portal where the host is prompted to download the Mobile Agent from Google Play (Android). • Latest Mobile Agent: Hosts with this operating system are required to download and install the highest version of the Mobile Agent availability Mobile Agent is downloaded from Google Play. See Mobile Agent on page 506.
Settings For Operating Systems Without Agents	This section provides a list of additional operating systems and allows you to select treatment for each one. For example, iPod devices could be set to None-Bypass indicating that no agent is necessary and allowing that device to connect to the network. Options for additional platforms include: • None-Deny Access: No agent is assigned and hosts are denied access to the network if they have the matching operating system. • None-Bypass: No agent is assigned but hosts are allowed to access the network if they have the matching operating system. Use Set all to None-Bypass or Set all to None-Deny Access to modify settings for all additional platforms at once. The last platform labeled Other is used as a catch-all for devices with new or unsupported operating systems. Any platform not listed in the Policy, is treated as specified by the setting associated with Other.
Override Scan Result Actions	Perform an action based upon the scan result: - On Success - On Warning - On Failure

Field	Definition
	Action options: - Do Nothing (Default) - Select an existing Action - Create new Action (see https://docs.fortinet.com/document/fortinac-f/7.6.0/administration-guide/939407/add-or-modify-an-action) Note: If the configured action does not apply to the host itself (example: disable port), the host health status will remain at "initial".

Configurations in use

To find the list of FortiNAC features that reference a specific endpoint compliance configuration, select the Configuration from the **Endpoint Compliance Configurations** view and click **In Use**. A message is displayed indicating whether or not the configuration is associated with any other features. If the configuration is referenced elsewhere, a list of each feature that references the configuration is displayed.

Delete a configuration

If a configuration is in use by another feature in FortiNAC, it cannot be deleted. A dialog displays with a list of the features in which the configuration is used. Remove the association between the configuration and other features before deleting the configuration.

1. Click **Policy & Objects**.
2. Expand **Endpoint Compliance**.
3. Select **Configuration** from the menu.
4. Select the configuration to be removed.
5. Click **Delete**.
6. Click **OK** to confirm that you wish to remove the configuration.

Chaining configuration scans

When advanced scan controls is enabled for an endpoint compliance configuration, you can map a security action containing **Run Endpoint Compliance Configuration** to scan results.

The **Run Endpoint Compliance Configuration** activity will run scans for additional endpoint compliance configurations. This allows further scans to be run on hosts when additional levels of access are needed. For example, if the host is part of a group requiring access to a secure VLAN, you can run additional scans the host must pass to be allowed onto this area of the network. Access is determined by the highest level scan that the host passes.

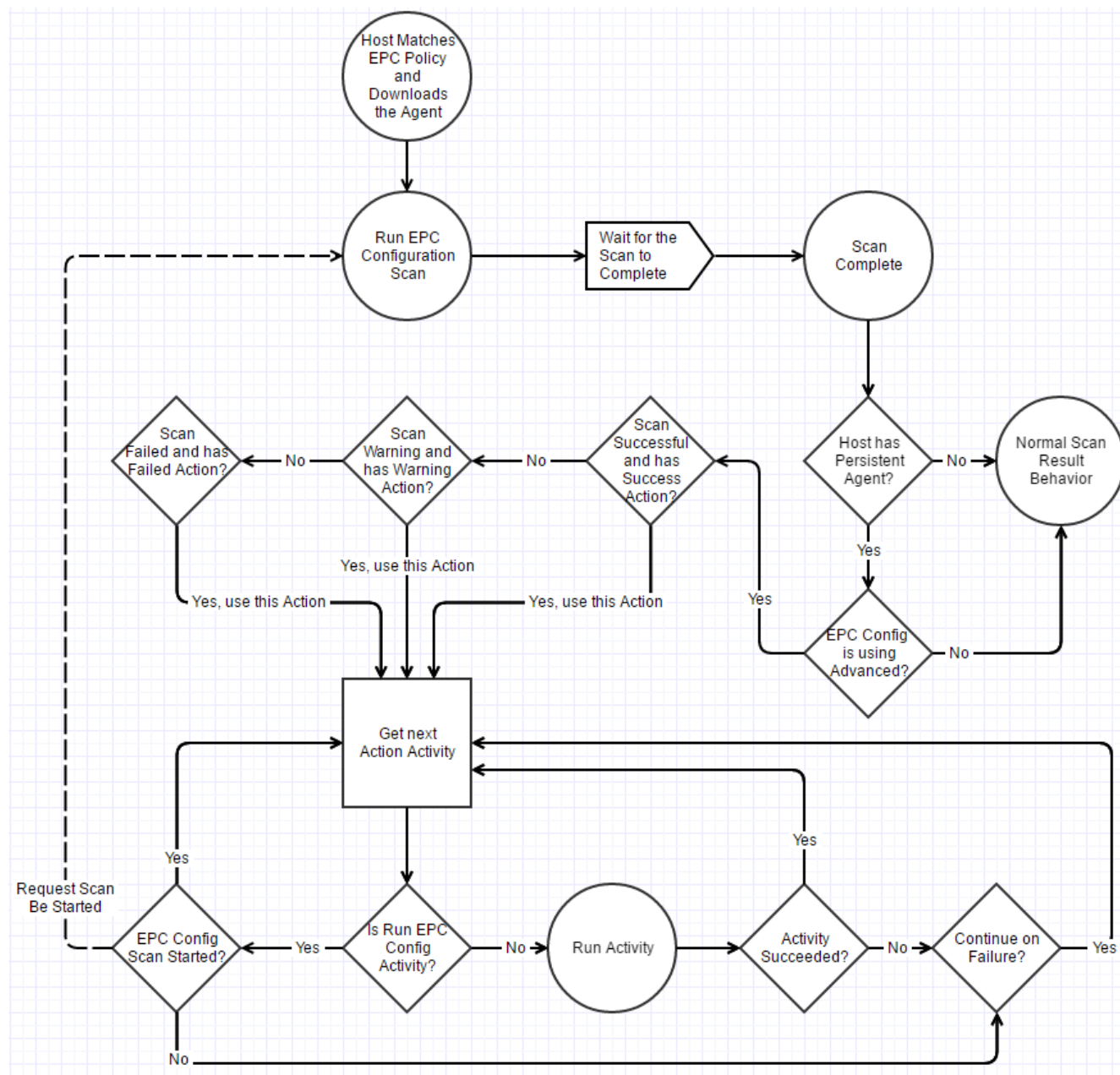
When a host is authenticated and matches an endpoint compliance policy, the endpoint compliance configuration scan is run. When the action is taken based on the scan results, if the **Run Endpoint Compliance Configuration** activity is performed and the endpoint compliance configuration scan starts successfully, the action moves to the next activity in the list while the endpoint compliance configuration scan is running.

If the endpoint compliance configuration scan does not successfully start, additional activities are only performed if **On Activity Failure** is set to **Continue Running Activities**.

There is no limit on the number of actions that can be run based on scan results.

The Persistent Agent must be installed on the host.

To enable and configure advanced scan controls, go to **Policy & Objects**. Click **Endpoint Compliance > Configuration**, and then click **Add** or select an existing configuration and click **Modify**.



Scans

The **Scans** view allows you to configure network scans or sets of rules that are used to scan hosts for compliance. Scans are included in endpoint compliance configurations that are paired with user/host profiles, which form endpoint compliance policies. When a host is evaluated and requires an endpoint compliance policy, FortiNAC goes through the list of policies and compares user and host information to the associated user/host profile. When a match is found, the endpoint compliance configuration inside the policy is applied to the host. That configuration contains the scan and agent information used to evaluate the host.

Scans typically consist of lists of permitted operating systems and required antivirus software. In addition, custom scans can be created for more detailed scanning such as searching the registry for particular entries, searching the hard drive for specific files, or verifying that hotfixes have been installed. Individual scans can be scheduled to run at regular intervals if your organization requires frequent rescans.

The results of a scan are stored on **Logs > Scan Results** page.

When you scan hosts, the agent first checks to see if a required item is installed and then proceeds to scan for additional details about that item. For example, if the host is required to run Windows 10 and that operating system is not installed, the agent does not check to see if the updates have been installed. Scan results, therefore, are reduced because needless scans are minimized. In the scan results, the host fails only for not having the operating system.

Using the example from the table shown above, the Agent ignores items that are not checked or selected. With this agent, you would achieve the following results.

- Operating system 1 requires antivirus 3. The agent does not test to see that antivirus 1 and 2 are not installed, therefore, the host cannot pass the scan unless it has operating system 1 with antivirus 3.
- Operating system 2 requires either antivirus 1 or antivirus 2. The agent does not test for antivirus 1.
- Operating system 3 requires either antivirus 1, antivirus 2, or antivirus 3.

Settings

Field	Definition
Scan Name	Each scan must have a unique name.
Remediation	Indicates when the host is moved to Remediation. Options include: On Failure: Host is moved to remediation immediately after failing a scan. Delayed: Host is moved to remediation after a user specified delay if the reason for the scan failure has not been addressed. Audit Only: Host is scanned and a failure report is generated, but the host is never moved to remediation.
Scan On Connect	Indicates whether this option is enabled or disabled. Scan On Connect forces a rescan every time the host assigned this scan connects to the network. See Scan on connect on page 544 . This option only affects hosts running the Persistent Agent.

Field	Definition
Renew IP (Supported by Dissolvable Agent Only)	Indicates whether the Renew IP option is enabled or disabled. When this option is enabled, it causes the Dissolvable Agent to actively release and renew the IP address of the host after it has completed its scan. The Renew IP option is only supported on Windows and macOS.
Scan Failure Link Label	Label displayed on the failure page when a network user's PC has failed a scan. If no label is provided, the scan name is used. The label or scan name is a link that takes the user to a page indicating why the PC has failed the scan.
Agent Order Of Operations Remediation = On Failure	This set of options is available only when Remediation is set to On Failure. Determines the order in which the agent performs its tasks. Choose one of the following: Scan Before Registering: The host downloads the Agent and is scanned in the registration network before being registered. If the scan fails you must choose one of the following: • Do not Register, Remediate: Host remains a Rogue and stays in the registration network until it passes the scan. Note the host will not be marked "at risk." Default setting. • Register and mark At Risk: The host is registered immediately after the scan and then moved to Quarantine.  Persistent Agent always registers and marks at risk. Register, then Scan (if the scan fails, Remediate): The host does not download an agent in the Registration network. Instead, the host is registered and moved to Quarantine to download the Agent and be scanned.
Agent Order Of Operations Remediation = Delay or Audit Only	The option below is available only when Remediation is set to Delay or Audit Only. If scan fails - Register or Remediate: If the host fails a scan, a web page with a Register option and a Remediate option is displayed to the user. If the user chooses the Remediate option, the host is placed in remediation and the user must correct all issues and rescan. If the user chooses the Register option, the host is placed in production. The user can correct all of the issues and re-run the Agent.
Patch URL	URL for the web page to be displayed when a host using the Dissolvable Agent fails the scan. This web page allows the user to download the agent and rescan after addressing the issues that caused the failure. Hosts using the Persistent Agent have the agent installed and do not use this page.
Root Detection	Indicates whether this option is enabled or disabled. If enabled, rooted mobile devices are not allowed to register. Mobile Agent devices determines whether or not the device has been rooted. Rooting is a process allowing users of devices running the Android operating system to attain privileged control (known as "root access") within Android's subsystem.

Field	Definition
Last Modified By	User name of the last user to modify the scan.
Last Modified Date	Date and time of the last modification to this scan.
Right click options	
Copy	Copy the selected Scan to create a new record.
Delete	Deletes the selected Scan. Scans that are currently in use cannot be deleted.
In Use	Indicates whether or not the selected Scan is currently being used by any other FortiNAC element. See Scans in use on page 555 .
Modify	Opens the Modify Scan window for the selected Scan.
Schedule	Opens the Schedule Policy view for the selected scan and allows you to add a schedule for host rescans using that Scan. See Schedule a scan on page 556 .
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746 .
 You must have permission to view the admin auditing log. See Add an administrator profile on page 139 .	
Buttons	
Custom Scans	Opens the Custom Scan Configuration window which allows you to add, remove or modify custom scans. Custom scan can be added to policies for more detailed host scans. See Custom scans on page 560 .
Schedule	Opens the Schedule Policy view for the selected scan and allows you to add a schedule for host rescans using that Scan. See Schedule a scan on page 556 .

Scan on connect

FortiNAC allows you to configure Scans that scan hosts each time they connect to the network. The Scan on Connect option is enabled on individual Scans. You may have hosts that are scanned each time they connect and hosts with a different Scan that are scanned periodically.



Scan on Connect can only be used on registered hosts that have the Persistent Agent installed. If you are using the Dissolvable Agent, this option is ignored.

When a host connects to the network, FortiNAC determines which endpoint compliance policy should be applied to this host based on the criteria in the associated user/host profile. If a registered host has the Persistent Agent installed and Scan on Connect is enabled for the Scan that applies to this host, then the host is scanned. When the host disconnects from the network, the Persistent Agent modifies that host's Scan on Connect status to indicate that the host should be scanned again the next time it connects. If the host has more than one interface, such as wired and wireless, the host is scanned regardless of which one is used.



A rescan happens any time FortiNAC detects that the host has come online and the agent has communicated with the server, such as when a switch sends a linkdown/linkup trap.

To enable Scan on Connect you must go to the Scans window, select the appropriate Scan and enable the option. See [Add or modify a scan on page 547](#) for step-by-step instructions on creating a Scan and enabling Scan on Connect.

Scan hosts without enforcing remediation

Hosts who are in Remediation are denied network access until they comply with the requirements of the Scan used to evaluate them. FortiNAC can scan hosts on the network without placing them in Remediation. This allows the administrator to determine host state or test new endpoint compliance policies without interrupting network users as they work. To scan hosts without enforcing remediation you can disable the Quarantine switching option in FortiNAC Properties. Disabling quarantine VLAN switching affects all hosts. However, you may need to scan selected hosts with no repercussions.

Two options have been provided to allow you to scan selected hosts without forcing "at risk" hosts into Remediation, Audit Only and Forced Remediation Exceptions group. You can use either one or both of these options. They work independently of each other. Audit Only controls remediation based on the scan applied. The Forced Remediation Exceptions group controls remediation based on group membership regardless of the scan used to evaluate the hosts.

Audit only

When the Audit Only option on a scan is enabled, hosts are scanned and the results of the scan are stored. Hosts that fail the scan are never marked "at risk" and therefore are not forced into Remediation or Quarantine. Administrators can then review all of the scan results and address issues of non-compliance without blocking users from the network.

Audit Only affects only those hosts evaluated by the scan in which Audit Only is enabled. If you have other scans with Audit Only disabled, hosts evaluated by those scans who fail are forced into Remediation. Using this option you can decide to force some groups of hosts into remediation while leaving others on the network. For example, you could have a scan for your executive staff that has Audit Only enabled and a different scan for administrative staff that has Audit Only disabled. Executives that fail a scan would continue to work without disruption, while administrative staff that fail a scan would be forced to remediate.

1. Click **Policy & Objects**.
2. Expand **Endpoint Compliance**.
3. Click **Scans**.
4. Select an existing scan to modify or create a new one.
5. On the **Add or Modify Scan** window go to the **Scan Settings** section and enable **Audit Only** under the **Remediation** drop-down.

See [Add or modify a scan on page 547](#) for additional information.

Forced remediation exceptions group

When hosts are placed in this group, they are evaluated by the scan that corresponds to them. See [Policy assignment on page 458](#). Results of the scan are stored and hosts who fail are marked "at risk". Hosts in this group are never forced into remediation no matter which scan they fail. To prevent selected hosts from being forced to remediate, add them to this group.

The Forced Remediation Exceptions group is a system group that has already been created. System groups cannot be removed only modified. See [System groups on page 851](#) and [Modify a group on page 846](#).

Delayed remediation

Delayed remediation allows you to scan hosts on your network, notify the user if the host has failed the scan and delay placing the host in the remediation VLAN for a specified number of days. This process gives the host's owner time to rectify the issues that triggered the failed scan and rescan without being removed from the network. If the user does not take care of the issues that caused the failure and successfully rescan the host by the time the specified delay has elapsed, the host is placed in remediation and cannot access the network.

Implementation

To implement Delayed Remediation, first implement the settings for endpoint compliance. See [Implementation on page 489](#).

- This feature works with any agent (Passive Agent, Persistent Agent, or Dissolvable Agent). If you choose to use this feature with the Dissolvable Agent, note the following:
 - Using the Dissolvable Agent, delayed remediation can only be implemented during the registration process where the host is provided a link to the Dissolvable Agent. If the host fails, it is marked as Pending - At Risk, but can register and move to the production VLAN. The Dissolvable Agent remains on the host until all issues have been resolved and the host has been rescanned.
 - If you set up scheduled rescans for hosts, using Delayed Remediation does not prevent the scheduled rescan from marking the host "At Risk" at the scheduled interval. Therefore, it is recommended that you use Proactive Scanning with the Dissolvable Agent instead of Delayed Remediation. Proactive Scanning allows a user to rescan a host prior to a scheduled required rescan and if the host fails it is not marked "at risk" until the date of the scheduled rescan. See [Schedule a scan on page 556](#).

To rescan the user must open a browser and navigate to the following:

`https://<Server or Application Server>/remediation`

The FortiNAC Server or Application Server in the URL can be either the IP address or Name of the server that is running the captive portal.

- Modify existing scans or create new ones and set the Delayed Remediation option for the number of days the host should be allowed to continue on the network after failing a scan. The default setting for Delayed Remediation is 0 days or no delay. See [Add or modify a scan on page 547](#).
- If a host has already failed a scan with a Delayed Remediation setting and the delay setting is changed on the Scan, it does not change the delay for the associated host. For example, if Host A is scanned, fails Scan A and is assigned a delay of 2 days, changing Scan A to a delay of 5 days does not alter the delay for Host A. It remains 2 days.
- Configure events and alarms to notify you when a host is affected by the Delayed Remediation setting. See [Enable and disable events on page 773](#). Events include:
 - **Host Pending At Risk:** Indicates that a host has failed a scan that has a Delayed Remediation set and has been set to Pending At Risk.
 - **Host Security Test - Delayed Failure:** A host has failed a scan and the scan has been set to Failure Pending in the Host Properties Health Tab.

Process

Below is a sample of the process FortiNAC goes through when Delayed Remediation is enabled.

1. A host connects to the network and is scanned by an agent with Scan A that has a 3 day delay configured.
2. The host fails the scan for antivirus.
3. A failure page indicating the reason for the failure is displayed on the host.
4. A Delayed Remediation record is created for this host and Scan A, which was used to scan the host.
5. The host's status is set to Pending At Risk.
6. On the Host Properties - Health Tab the scan for Scan A is set to Failure Pending.
7. The host remains on the production network and is not sent to the remediation VLAN.
8. After one day the host connects in the Library and is scanned by an agent with Scan B that has a 5 day delay configured.
9. The host fails the scan for operating system.
10. A failure page indicating the reason for the failure is displayed on the host.
11. A second Delayed Remediation record is created for this host and Scan B.
12. The host status remains Pending At Risk.
13. On the Host Properties - Health Tab the scan for Scan B is set to Failure Pending.
14. The user corrects the antivirus issue and rescans with Scan A.
15. The Delayed Remediation record for this host and Scan A is removed.
16. On the Host Properties - Health Tab the scan for Scan A is set to Success.
17. The host's status remains Pending At Risk because the user has not corrected the operating system issue and rescanned for Scan B.
18. Five days elapse and the user still has not corrected the operating system issue and rescanned for Scan B.
19. The host is marked At Risk but it is not moved to the Remediation VLAN because Scan B is not the scan that currently applies to the host. Scan B will apply to the host if the host ever reconnects in the Library.
20. On the Host Properties - Health Tab the scan for Scan B is set to Failure.
21. The Delayed Remediation record for this host and Scan B is removed.
22. The host continues on the production network.
23. If the host ever reconnects in the Library, the host will be placed in Remediation. The User will have to resolve the operating system issue and rescan the host for Scan B.

Each host failure and delay record is treated individually. Passing one scan and associated delay, does not remove failures for other scans and corresponding delays. However, if a failed scan does not apply to the host, the host will not be sent to remediation. Refer to [Host health and scanning on page 224](#).

Add or modify a scan

Use the Add or Modify Scan dialog to configure scan settings. Settings are divided into two tables. The first table details the fields on the General tab and the second details the Categories available under the remaining tabs.

1. Select **Policy & Objects**.
2. Expand **Endpoint Compliance**.
3. Click the **Scans** option to select it.
4. On the Scans View, click **Add** to add a new scan or select an existing Scan and click **Modify**.
5. Enter data in the fields as needed. See the **Settings** table below for information on each field.
6. For each **operating system** tab, there is a drop-down menu of categories that can be set, such as antivirus settings. Instructions for configuring each category are contained in the Scan Configuration Settings - Categories table.

7. The **Summary** tab provides an overview of the entire scan configuration for your review.
8. Click **OK** to save the scan.

Settings - general tab

Field	Definition
Scan Name	Each scan must have a unique name.
Scan settings	
Scan On Connect (Persistent Agent Only)	Forces a rescan every time the host assigned this scan connects to the network. This option only affects hosts running the Persistent Agent. See Scan on connect on page 544 .
Renew IP (Supported Dissolvable Agent Only)	Indicates whether the Renew IP option is enabled or disabled. When this option is enabled, it causes the Dissolvable Agent to actively release and renew the IP address of the host after it has completed its scan. The Renew IP option is only supported on Windows and macOS.
Root Detection (Mobile Agent Only)	The Mobile Agent determines whether or not the device has been rooted. Rooting is a process allowing users of devices running the Android operating system to attain privileged control (known as "root access") within Android's subsystem. If enabled, rooted mobile devices are not allowed to register. If disabled, devices suspected of being rooted are allowed to register and (Rooted) is appended to the operating system information displayed in the Host View. If the agent detects that device has been altered, a Potential Rooted Device event is generated.
Remediation - On Failure	If enabled, the host is scanned and the information associated with the scan is recorded. If the host fails the scan, the user must resolve all of the issues for which the host failed and rescan before being allowed on the network. Agent Order Of Operations: This set of options is available only when Remediation is set to On Failure. Determines the order in which the agent performs its tasks. Choose one of the following: Scan Before Registering: The host downloads the Agent and is scanned in the registration network before being registered. If the scan fails you must choose one of the following: • Do not Register, Remediate: Host remains a rogue and stays in the registration network until it passes the scan. Note the host will not be marked At Risk. • Register and mark At Risk: The host is registered immediately after the scan and then moved to quarantine. • Register, then Scan (if the scan fails, Remediate): The host does not download an agent in the registration network. Instead, the host is registered and moved to quarantine to download the Agent and be scanned.
Remediation - Delayed	Hosts who fail this scan are set to Pending at Risk for the number of days indicated in the Remediation Delay field. Hosts set to Pending at Risk are not placed in remediation until the number of days indicated has elapsed. The user is notified of the failure immediately.

Field	Definition
	Changes to this setting do not affect hosts that are already marked as Pending At Risk. If a host was set to a delay of 3 days and you change the Remediation Delay field to 5 days, the host remains at a delay of 3 days. Hosts scanned after the change will use the 5 day setting. Agent Order Of Operations: If scan fails - Register or Remediate: If the host fails a scan, the Persistent Agent displays a message stating that the host is at risk. Click the message to display information about the scan. The host is automatically registered. The Dissolvable Agent displays the results of the scan. You can choose to rescan or register. When the host is registered, the host is placed in production. The user can correct all of the issues and re-run the Agent.
Remediation - Audit Only	If enabled, the host is scanned and the information associated with the scan is recorded. If the host fails the scan, it is not marked "at risk". Therefore, it is not forced into Remediation and can continue using the network. The administrator can review the scan results and take corrective action without disrupting users on the network. Agent Order Of Operations: If scan fails - Register or Remediate: If the host fails a scan, a web page with a Register option and a Remediate option is displayed to the user. If the user chooses the Remediate option, the host is placed in remediation and the user must correct all issues and rescan. If the user chooses the Register option, the host is placed in production. The user can correct all of the issues and re-run the Agent.
Remediation	If On Failure is enabled, the host is scanned and the information associated with the scan is recorded. If the host fails the scan, the user must resolve all of the issues for which the host failed and rescan before being allowed on the network. If Delayed is enabled, hosts who fail this scan are set to Pending at Risk for the number of days indicated in the Remediation Delay field. Hosts set to Pending at Risk are not placed in remediation until the number of days indicated has elapsed. The user is notified of the failure immediately. If Audit Only is enabled, the host is scanned and the information associated with the scan is recorded. If the host fails the scan, it is not marked At Risk. Therefore, it is not forced into remediation and can continue using the network. The administrator can review the scan results and take corrective action without disrupting users on the network.

Field	Definition
Agent Order of Operations	When Remediation is set to On Failure: Determines the order in which the agent performs its tasks. Choose one of the following: • Scan Before Registering: The host downloads the Agent and is scanned in the registration network before being registered. If the scan fails you must choose one of the following: • Do not Register, Remediate: Host remains a Rogue and stays in the registration network until it passes the scan. Note the host will not be marked "at risk." Default setting. • Register and mark At Risk: The host is registered immediately after the scan and then moved to Quarantine.  Persistent Agent always registers and marks at risk. Register, then Scan (if the scan fails, Remediate): The host does not download an agent in the Registration network. Instead, the host is registered and moved to Quarantine to download the Agent and be scanned. When Remediation is set to Delayed or Audit Only: If scan fails - Register or Remediate: If the host fails a scan, a web page with a Register option and a Remediate option is displayed to the user. If the user chooses the Remediate option, the host is placed in remediation and the user must correct all issues and rescan. If the user chooses the Register option, the host is placed in production. The user can correct all of the issues and re-run the Agent.
Portal page settings	
Label For Scan Failure Link	Label displayed on the failure page when a network user's PC has failed a scan. If no label is provided, the scan name is used. The label or scan name is a link that takes the user to a page indicating why the PC has failed the scan.
Instructions For Scan Failure	If a host has failed a scan, the user must remedy the issue and rescan. This field allows you to provide the user with a brief set of instructions.
Patch URL For Dissolvable Agent Re-Scan	URL for the web page to be displayed when a host using the Dissolvable Agent fails the scan. This web page allows the user to download the agent and rescan after addressing the issues that caused the failure. Hosts using the Persistent Agent have the agent installed and do not use this page. Set this to /remediation To rescan the user must open a browser and navigate to the following: <a href="https://<Server or Application Server>/remediation">https://<Server or Application Server>/remediation The FortiNAC Server or Application Server in the URL can be either the IP address or Name of the server that is running the captive portal.

Field	Definition
In use by/Not currently in use	Indicates whether the scan is being used in user/host profile(s). When the scan is in use, click the link to view the user/host profile(s).

Settings - categories

For each operating system there is a Category drop-down that allows you to configure specific settings for categories such as antivirus. The table below outlines these settings.

Default parameter values for individual antivirus and operating systems packages are entered and updated automatically by the scheduled Auto-Def Updates. If the values have been manually edited, the Auto-Def Updates will not override those changes.

Removing a check mark from a selected option causes any underlying changes to be lost. For example, if you modified settings for AVG antivirus and then unselected it, those changes are lost.

Field	Definition
Antivirus	
Validation Options	• Any: Any one of the selected items must be present on the host to pass the scan. • All: All of the selected items must be present on the host to pass the scan.
Anti-Virus List	New antivirus software is continually being created. As new antivirus software becomes available, parameters for that software are made available as quickly as possible in FortiNAC. The default values for each antivirus program are entered automatically by the scheduled Auto-Def Updates feature. You should not need to modify these. Select one or more types of Anti-virus software to check for on the host. To set additional parameters for any of the selected antivirus programs, click the name of a program. A parameters window opens and displays all of the advanced options that can be set. Enter the custom parameter values for the selected program and click OK. See Antivirus parameters - Windows on page 581 or Antivirus parameters - macOS on page 585 for details on each parameter.
Preferred	Select the Preferred Anti-Virus from the drop-down list. If the host fails for all of the products selected for the scan, only the preferred item selected is displayed on the Failed Policy pages. If no Preferred product is selected, the list displayed on the Failed Policy pages contains a separate line for every product failure.
Custom scans	
Custom Scans List	Custom scans are user created scans that have been configured to scan hosts for things such as specific files, registry entries or programs. Custom scans must be created and saved before they can be included as part of a Security Policy. See Custom scans on page 560. When a Custom scan is added to a regular scan the custom scan is used across the board no matter what other options have been selected for the policy. Any host that is scanned with the regular scan is also scanned based on the custom scan. See Create a scan on page 561.

Field	Definition
	Custom scans can be added within a category, such as antivirus. For example, any host that has AVG Antivirus will be scanned using an associated custom scan. In this case, the custom scan is being used to enhance the scan for AVG Antivirus and it is not run on every host. See Scan categories on page 561 .
Operating systems	
Selection Options	• All: Marks every operating system with a check mark. • None: Removes the check mark from every operating system check box.
Operating Systems List	Scans for required or prohibited operating systems on hosts. Operating systems that are selected are required. See Operating system parameters - Windows on page 587 The Windows-2003-Server-x64 product has been removed. Use the Windows 2003 Server and Windows XP x64 products.
Preferred	Select the preferred operating system from the drop-down list. If the host fails for all of the products selected for the scan, only the preferred item selected is displayed on the Failed Policy pages. If no Preferred product is selected, the list displayed on the Failed Policy pages contains a separate line for every product failure.
Monitors	
Scan List	Allows you to run a custom scan with greater frequency than the regular scan with which it is associated. For example, the original scan may only run once a week, but you may have a custom scan that needs to run every half an hour. Instead of running the entire scan policy every half an hour you can choose to run only a custom scan. Select a custom scan and enter the frequency with which it should run. Performance degradation may occur if you select an interval less than every five (5) minutes. It is recommended that monitoring intervals be set to five (5) minutes or more.
Miscellaneous	
Validate	Products available for evaluation that are not antivirus or operating system Product Options (available for Windows and Mac-OS-X): McAfee-EPO Palo-Alto-GlobalProtect Microsoft-SCCM-2012-Client
Failed Policy Preferred Product	Select the Preferred product from the drop-down list. If the host fails for all of the products selected for the scan, only the preferred item selected is displayed on the Failed Policy pages. If no Preferred product is selected, the list displayed on the Failed Policy pages contains a separate line for every product failure.

Custom scan options - scan level

Custom scans can be enabled for a regular scan. When a host is checked for compliance with the regular scan, the custom scan is also checked. Before adding a custom scan to a security scan you must create the custom scan.

To enable a Custom scan for a security scan:

1. Click **Policy & Objects**.
2. Expand **Endpoint Compliance**.

3. Click the **Scans** option to select it.
4. Modify the scan that will use this custom scan.
5. Click either the **Windows**, the **macOS**, or the **Linux** tab.
6. Select **Custom** from the drop-down menu at the top of the window.
7. Select the check box next to the custom scan for the security scan.
8. Click **OK** to save your changes.

Custom scans options within a category level

Custom scans can be enabled for various categories within a security scan such as the antivirus or operating system requirements. When a host is checked for compliance with the security scan and one of the products within a category has a custom scan enabled, the custom scan is also used for hosts with the selected product. For example, if the security scan checks for the existence of AVG Antivirus and a custom scan has been associated with AVG, then hosts with AVG will also be scanned using the custom scan.

Before adding a custom scan to a security scan you must create the custom scan.

1. Click **Policy & Objects**.
2. Expand **Endpoint Compliance**.
3. Click the **Scans** option to select it.
4. Modify the security scan that will use this custom scan.
5. Click either the **Windows**, the **macOS**, or the **Linux** tab.
6. Click the **Category** drop-down on the Modify Scan view and select: antivirus, operating system, etc.
7. Click the specific item within the sub-category (i.e. product name).
8. Click the **Custom Scans** tab and select the custom scan to be applied to this sub-category.
9. Click **OK** to save the selected custom scan.
10. Click **OK** to save changes to the security scan.

Monitor custom scans



Script custom scans can't be used as a monitor.

This feature allows you to run a custom scan with greater frequency than the security scan with which it is associated. For example, the original security scan may only run once a week, but you may have a custom scan that needs to run every half an hour. Instead of running the entire security scan every half an hour you can choose to run only a custom scan.

Use the monitor feature to periodically test for a specific status on hosts running the Persistent Agent. Monitors use custom scans to check the host. A monitor you configure as part of a scan can be the same or different for each scan. Configure monitors for each platform (Windows, macOS, or Linux) separately.

Hosts associated with the security scan are checked at the interval period set in the monitor. The agent on the host sends a message to the server after each time period has passed, indicating whether the host has passed or failed the scan. If several monitors are set to 1 minute intervals, traffic to the server is increased. For example, if there are 10 monitors running every minute on 5,000 hosts, the server might see up to 50,000 messages a minute.

Even though monitors use custom scans which can be set to warning, monitors will not send warnings to hosts. Monitors can only pass or fail. Hosts that fail are marked at risk and placed in remediation.

Enabling a monitor for a custom scan automatically enables the custom scan. However, disabling a monitor will not disable the associated custom scan.

For example, you have created custom scan A but have not selected it within any security scan. When you select custom scan A in the Monitor list select a time period, the custom scan is enabled.

Monitors ignore the severity flag of a custom scan.

Monitor example

All users have been notified that peer-to-peer software is not tolerated on the network. A web page explaining this policy is located in the remediation area where the host is moved after failing the scan.

Actions taken:

- A custom scan for a prohibited process has been created to check for LimeWire, a peer-to-peer software program, running on the host. The custom scan includes the URL of the web page where the host browser will be directed if the host fails the custom scan.
- The monitor is set to 10 minutes for the custom scan.

Results:

- Every 10 minutes the agent checks the host to determine if LimeWire is running.
 - If LimeWire is not running, the agent sends a message to the server indicating that the host has passed the security scan.
 - If LimeWire is running, the agent sends a message to the server indicating that the host has failed the scan. The host is immediately moved to the quarantine VLAN and the browser redirected to the web page specified in the custom scan.

Set up a custom scan monitor

Before adding a custom scan to a security scan you must create the custom scan.

1. Click **Policy & Objects**.
2. Expand **Endpoint Compliance**.
3. Click the **Scans** option to select it.
4. Click the security scan name and click **Modify**. If the security scan does not exist, it needs to be added. See [Scans on page 542](#) for details on adding scans.
5. Click either the **Windows**, the **macOS**, or the **Linux** tab.
6. Click the **Category** drop-down and select **Monitors**.
7. Select the check box for the type of custom scan.
8. Select the time period that the agent waits before checking the host for compliance with the custom scan settings. The available intervals are every 15 seconds up to and including 1 minute, and every 5 minutes up to and including 1 hour.

Performance degradation may occur if you select a very short interval or if you select a large number of monitors. It is recommended that monitoring intervals be set to five (5) minutes or more.
9. Click **OK**.

Reset default antivirus values

Antivirus parameters contained in FortiNAC are updated weekly using the Auto-Def updates feature. This ensures that new version numbers and bug definition files for antivirus software that you require are taken into account when users' computers are scanned.

If you have manually edited any parameters associated with a particular antivirus software the Auto-Def update does not override your settings for that software. To reset antivirus to the default values and allow the Auto-Def updates feature to update parameters do the following:

1. Click **Policy & Objects**.
2. Expand **Endpoint Compliance**.
3. Click the **Scans** option to select it.
4. Select a scan and click **Modify**.
5. Click either **Windows** or **Mac**, whichever applies.
6. Select **Anti-Virus** from the **Categories** drop-down.
7. Uncheck the checkbox for the software for which you have modified settings.
8. Click **OK**.
9. Open the same scan again and navigate back to the software you unchecked.
10. Check the checkbox for the previously modified settings and click **OK**.
11. Repeat this process for each antivirus software that needs to be reset to defaults.
12. The next time the Auto-Def updates feature retrieves and installs an update, the antivirus software that you reset will accept the updated parameters.

Delete a scan

If a Scan is in use by another feature in FortiNAC, it cannot be deleted. A dialog displays with a list of the features in which the scan is used. Remove the association between the scan and other features before deleting the scan.

Deleting a scan automatically removes scheduled tasks for that scan.

1. Click **Policy & Objects**.
2. Expand **Endpoint Compliance**.
3. Click the **Scans** option to select it.
4. Click the scan to be removed.
5. Click **Delete**.
6. Click **OK** to remove the scan.

Scans in use

To find the list of FortiNAC features that reference a specific Scan, select the Scan from the Scans View and click **In Use**. A message is displayed indicating whether or not the Scan is associated with any other features. If the Scan is referenced elsewhere, a list of each feature that references the Scan is displayed.

Schedule a scan

When hosts that use the Persistent Agent or the Dissolvable Agent connect to the network, they are checked against an endpoint compliance policy. FortiNAC maintains a list of hosts that have passed the scan within the policy. When hosts that previously passed the scan connect to the network, they are given access.

To recheck the hosts and ensure continued compliance, schedule the scan to be run at specific intervals. The hosts are rechecked the next time the scheduled task for the scan runs. Only hosts that have a valid operating system listed in Host Properties are rescanned. Valid operating systems include Linux, Windows, and macOS.

You can add more than one scheduled task for each scan to check different groups of network hosts at various times. This prevents an excessive load on the system. These groups are subgroups of the original group targeted by the scan. For example, if the original scan was set to scan all staff in the Building A group, the scheduled scan could target staff in subsets of the Building A group. Subsets would be created by placing staff from the Building A group into smaller groups. Then, the 1st floor group could be scanned on Mondays, the 2nd floor group could be scanned on Tuesdays, etc.

If FortiNAC has lost contact with the host's Persistent Agent, the host cannot be scanned. Offline hosts will be rescanned when they come back online.

1. Click **Policy & Objects**.
2. Expand **Endpoint Compliance**.
3. Click the **Scans** option to select it.
4. Click the scan to be scheduled.
5. Click **Schedule**. The Schedule Rescan of Agents window opens. Any existing scheduled tasks appear in the window.
6. Click **Add**.
7. Use the information in the table below to configure your schedule.

Field	Definition
Task	
Scan Name	Name of the scan that will be used to rescan hosts.
Schedule Task Name	Each task for the selected scan must have a unique name.
Target Agent Types	Type of agent the hosts are using: all, Dissolvable Agent, or Persistent Agent.
Host Group	If selected, indicates the group of hosts that will be checked for scan compliance when this scheduled task runs. See Groups on page 843 for information on creating groups. This group of hosts must be contained within the set of hosts targeted in the original scan.
Security And Access Attribute	If selected, filters hosts for rescan based on a field in the user record with matching data in the LDAP or Active Directory. This group must be the same as or a subset of the group targeted in the original scan.
 If the Group option and the Security and Access Attribute option are both selected, the host must be a member of the group selected and the user must have a matching Security and Access Attribute value in order to be scanned.	

Field	Definition
	If neither the Group option nor the Security and Access Attribute option are selected, all of the hosts targeted by the original scan are scanned.
	Scans can be used in multiply policies, therefore, the set of hosts to be scanned could be quite large.
Schedule	
Status	Indicates whether the scheduled task is current enabled or disabled.
Schedule Interval	How often the scheduled task is to run. Enter a number and select Days, Hours, or Minutes from the drop-down list.
Next Scheduled Time	The next date/time to run the scheduled task. Enter in the format MM/DD/YY HH:MM AM/PM
Modify Schedule	Opens the Modify Scheduled Activity dialog where you can configure the scan's schedule.
Proactive scanning	
Proactive Scanning	See the section below for additional information.

8. Click **Modify Schedule** to run the scheduled task automatically or on a fixed day.
 - To run the task automatically, select Repetitive Task to select the rate at which you wish to run the task. For example, selecting a Repetition Rate of two days and the Next Scheduled Time of today at 1:00 PM means the task will run today at 1:00 PM, and will continue to run every two days at 1:00 PM.
 - To run the task on a fixed day and time, select Fixed Day Task and then select the day(s). The task will automatically run on the selected day(s) and time each week.
9. Click **Apply**.

Add proactive scanning to a scheduled scan

Within FortiNAC you can schedule scans to run automatically. Hosts using the Dissolvable Agent can initiate a rescan on the production network. When a rescan is successful, the host has extended the time before another scan is required.

For example, assume the schedule is set to rescan every Sunday. The user rescans his host at his convenience on Friday and passes the scan. When Sunday comes, FortiNAC checks the scan history and determines that this host has had a successful scan. This host is not forced to rescan nor is it marked at risk.

If the host fails the scan, the user is presented with a list of reasons for the failure. The host is not marked at risk at this time. If the user resolves the issues and rescans before the scheduled scan date, the host is never marked at risk and is not forced to rescan on Sunday. If the user does not resolve the issues and rescan, when the scheduled scan date arrives the host is either marked at risk or aged out of the database. The host cannot access the network until it has been successfully scanned or until the host is reregistered and then is successfully scanned.

To rescan the user must open a browser and navigate to `https://<Server or Application Server>/remediation`.

The FortiNAC Server or Application Server in the URL can be either the IP address or Name of the server that is running the captive portal.

Proactive scanning is enabled on the Schedule Rescan window. To provide your hosts access to the Dissolvable Agent, you can create a web page accessible from your network to download the Dissolvable Agent.

Scan results are central to FortiNAC's ability to determine when a host was last scanned. Scan results are removed based on the archive and purge schedule set up in FortiNAC properties. When configuring the archive and purge schedule be sure to make the interval long enough to allow the scan results to be used for Proactive Scanning. If the interval is too short, scan results will be purged too soon forcing all hosts to rescan regardless of when their last scan occurred. See [Database archive on page 977](#) for information on archive and purge settings.

Schedule a scan: proactive scanning

Users can proactively rescan their computers to re-assess their system with or without any impact to their At Risk status. This feature helps to decrease the load around the re-registration process or rescan intervals.

To rescan the user must open a browser and navigate to `https://<Server or Application Server>/remediation`.

The FortiNAC Server or Application Server in the URL can be either the IP address or Name of the server that is running the captive portal.

The time extension capability can not change a guest record's age-out time; time extensions only apply to standard hosts.

Use the options in the **Schedule Rescan** window to specify whether to apply a time extension if there is a successful scan history within the interval, and what actions to take if there is no scan history. For example if a host does not rescan proactively, the registered host can be set to age-out or be marked At Risk.

Once you have created a policy, do the following to configure the proactive scanning and specify subsequent actions.

Add proactive scanning to a scan schedule

1. Click **Policy & Objects**.
2. Expand **Endpoint Compliance**.
3. Click the **Scans** option to select it.
4. Select the scan to be scheduled.
5. Click **Schedule**. The **Schedule Rescan of Agents** window opens. Any existing scheduled tasks for the scan appear in the window.
6. Click **Add**.
7. For **Target**, select **Dissolvable**. Only hosts using the Dissolvable Agent can do a proactive scan.
8. For the **Proactive Scanning Option**, select **On**.
9. Click **Apply**.

In the example shown below, the **Scan History Interval** is set to one week. If hosts have successfully passed a scan during the week prior to the time and date specified in the **Next Scheduled Time** field, their expiration time is extended by one week and they will remain on their production network. If they do not have a successful scan within the previous week, they are marked at risk and moved to remediation to be rescanned.

Settings

Field	Definition
Task	
Scan Name	Name of the Scan that will be used to rescan hosts.
Schedule Task Name	Each task for the selected policy must have a unique name.
Target Agent Types	Type of agent the hosts are using: all, Dissolvable Agent, or Persistent Agent.
Host Group	If selected, indicates the group of hosts that will be checked for scan compliance when this scheduled task runs. See Groups on page 843 for information on creating groups. This group of hosts must be contained within the set of hosts targeted in the original policy.
Security And Access Attribute	If selected, filters hosts for rescan based on a field in the user record with matching data in the LDAP or Active Directory. This group of must be the same as or a subset of the group targeted in the original policy.
	If the Group option and the Security and Access Attribute option are both selected, the host must be a member of the group selected and the user must have a matching Security and Access Attribute value in order to be scanned.
	If neither the Group option nor the Security and Access Attribute option are selected, all of the hosts targeted by the original scan are scanned.
	Scans can be used in multiply policies, therefore, the set of hosts to be scanned could be quite large.
Schedule	
Schedule Interval	How often the scheduled task is to run. Enter a number and select Days, Hours, or Minutes from the drop-down list.
Next Scheduled Time	The next date/time to run the scheduled task. Enter in the format MM/DD/YY HH:MM AM/PM
Pause	When selected, the scheduled task is paused and will not run automatically. Go to the Scheduler View and run the task manually. See the Scheduler on page 857 for more information.
Proactive scanning	

Field	Definition
Proactive Scanning	Select On . If you select Off, the hosts are placed in Quarantine when the scheduled task runs.
Scan History Interval (previous)	Interval of time the previous scan history is considered valid.
No Scan History Found	If the host has not been successfully scanned within the scan history interval, you have the option of marking the host at risk or aging the record. If you select At Risk, the host is moved to Quarantine to be rescanned. If you select Age Record, the host is deleted and must be re-registered to regain network access.
Scan History Found	If the most recent scan in the scan history is a successful scan for the host and is within the scan history interval, you have the option of selecting No Action or Extend Time. Select No Action to let the account remain with the existing expiration date and time. If the system takes no action, the host is forced to rescan when the expiration date and time are met even if the host has a successful scan prior to the expiration date and time. Select Extend Time to specify a period in Extend Expiration Date (the next field).
Extend Expiration Time	If Extend Time is selected and the host has had a successful scan within the Scan History Interval, the host's expiration time is extended by this amount.

Custom scans

Scans are configured to evaluate hosts connecting to the network. These scans search the host computer for things such as antivirus software or a particular version of an operating system. The categories within which the scan can search are fairly broad. To scan for very specific items, such as a file on the hard drive or a patch, you must create custom scans and then link custom scans to a general Scan.

The severity level set in the custom scan determines how the host is treated when it fails a custom scan. Levels can be set to deny the host access to the network or to just send a warning. See [Severity level on page 569](#) for additional details.

Custom scans that are associated with a scan can be configured to run at more frequent intervals than the Scan itself by setting up a Monitor in the Scan. This requires that the host have the Persistent Agent installed.

In addition to running a custom scan on any host that is evaluated by the associated Scan, you can use custom scans to refine or enhance other Scans. For example, if you have set up a Scan to check hosts for one of the following antivirus programs: AVG 8.5, Kaspersky, or Norton. Within the Kaspersky setting you can add a custom scan to search for a version that must be installed. This custom scan will not be run for hosts using AVG 8.5 or Norton. It will be run for hosts using Kaspersky.

Custom scans are created differently depending on the operating system on which they will run. You must create separate custom scans for each operating system.

When hosts fail a custom scan, they are redirected to the web page designated within the custom scan configuration. These web pages are not provided as part of the portal configuration. They must be created and stored on your FortiNAC appliance in the following directory: `/bsc/Registration/registration/site`

Within the directory listed above there are other web pages that might serve as a template for the custom scans web pages. One option is to copy the `antivirus.jsp` file to a new name and edit the text within that file to accommodate your custom scans.

User created web pages that display when a host fails a custom scan are now stored in `/bsc/Registration/registration/site`. If you are using Portal Version 1 and have legacy pages that are stored in `/bsc/Registration/registration/sma`, you do not need to move them to the new directory, they will continue to display to hosts as needed.



Custom Scans behavior with FortiNAC manager

An ECC custom scan is never automatically deleted during a sync operation from the Manager; they are only marked as non-global on the pod during a sync, if the ECC custom scan was deleted on the Manager.

The intentional behavior is to not delete them from the pod after they have been deleted from the Manager, then the Manager sync'd to the pod. The custom scans remain on the pod, but they are not marked as global; thus they're able to be deleted, if desired, in a second step.

Create a scan

Custom scans can be enabled for a regular scan. When a host is checked for compliance with the regular scan, the custom scan is also checked. Before adding a custom scan to a security scan you must create the custom scan. See [Windows Custom Scan on page 570](#), [macOS on page 562](#), or [Linux on page 565](#).

To enable a Custom scan for a security scan:

1. Click **Policy & Objects**.
2. Expand **Endpoint Compliance**.
3. Click the **Scans** option to select it.
4. Modify the scan that will use this custom scan.
5. Click either the **Windows**, the **macOS**, or the **Linux** tab.
6. Select **Custom** from the drop-down menu at the top of the window.
7. Select the check box next to the custom scan for the security scan.
8. Click **OK** to save your changes.

Scan categories

Custom scans can be enabled for various categories within a security scan such as the antivirus or operating system requirements. When a host is checked for compliance with the security scan and one of the products within a category has a custom scan enabled, the custom scan is also used for hosts with the selected product. For example, if the security scan checks for the existence of AVG Antivirus and a custom scan has been associated with AVG, then hosts with AVG will also be scanned using the custom scan.

Before adding a custom scan to a security scan you must create the custom scan. See [Windows Custom Scan on page 570](#) or [macOS on page 562](#).

1. Click **Policy & Objects**.
2. Expand **Endpoint Compliance**.
3. Click the **Scans** option to select it.
4. Modify the security scan that will use this custom scan.
5. Click either the **Windows**, the **macOS**, or the **Linux** tab.
6. Click the **Category** drop-down on the Modify Scan view and select: antivirus, operating system, etc.
7. Click the specific item within the sub-category (i.e. product name).
8. Click the **Custom Scans** tab and select the custom scan to be applied to this sub-category.
9. Click **OK** to save the selected custom scan.
10. Click **OK** to save changes to the security scan.

macOS

The custom scans feature allows you to search host computers for very specific information. Custom scans must be created separately for different operating systems. Within each operating system, there are different types of scans that can be created. Refer to **Add A macOS Custom Scan** below for a list of scan types and general instructions on adding scans. Refer to the instructions for each scan type for field level information. You can modify or remove the scans at any time. When a custom scan is modified, it affects any existing general scans that use that custom scan.

Add a custom scan

1. Click **Policy & Objects**.
2. Expand **Endpoint Compliance**.
3. Click the **Scans** option to select it.
4. Click **Custom Scans**.
5. Select **Add**.
6. Select **macOS** from the **Operating System** drop-down list.
7. Select the type of scan desired. Each scan type has a special set of fields that are specific to that type. Use the table below for settings.

Scan Type	Description
File	Test for the existence of a specific file on the host. See File scan settings on page 563 .
Package	Test for a existence of a specific installer package on the host. An inclusive range of macOS Versions can be specified for this scan. See Package scan settings on page 563 .
Processes	Test for the existence of a specific process. See Processes scan settings on page 564 .
Prohibited-Processes	Test for the existence of a specific prohibited process. See Prohibited processes scan settings on page 565 .

8. Enter the **Name** for the custom scan.
9. Enter the information for the custom scan.

10. Click **OK**.
11. The name of the custom scan will now appear in the **Custom Scans** section for each macOS scan and can be selected as part of the creation or modification of the general scan parameters.

File scan settings

To create a custom scan for a specific file, enter the information shown in the table below into the custom scan window after selecting the File scan type.

Scan Parameter	Description
Label	This label appears in the Results page information to identify which scan the host failed.
Severity	The severity of the failure if the file is not on the host. If you select Required and the file does not exist, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See Severity level on page 569 for more details.
File Name	The name of the file being checked for on the host.
Starting Path	The search for the file starts with the directory indicated here and includes all sub-directories and files. Important: Use the forward slash (/) to delimit directory names. Do NOT use a colon (:).
Web Address	The URL of the page with information regarding this file. If entered, this link appears on the Results page. This is a user created web page. It must be stored in: <code>/bsc/Registration/registration/site</code> When completing this field you must enter part of the path for the page not just the page name, such as: <code>site/pagename.jsp</code>
Prohibit this product	If the file is found and this is set to true, the host fails the scan for a prohibited product. Default = false.

Package scan settings

To create a custom scan for a specific installer package, enter the information shown in the table below into the custom scan window after selecting the Package scan type.

Use this custom scan to check whether particular updates or patches have been applied to the host.



If the package name is installed on a host with an OS version outside the range, the host will pass the scan.

Scan Parameter	Description
Label	This label appears in the Results page information to identify which scan the host failed.
Severity	The severity of the failure if the package is not on the host. If you select Required and the package does not exist, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See Severity level on page 569 for more details.
Package Name	name.pkg The name of the installer package being searched for on the host. The custom scan searches the /Library/Receipts directory for install receipts.
Minimum macOS Version	The inclusive minimum version of the macOS software.
Maximum macOS Version	The inclusive maximum version of the macOS software.
Web Address	The URL of the page with information regarding this installer package. If entered, this link appears on the Results page. This is a user created web page. It must be stored in: /bsc/Registration/registration/site When completing this field you must enter part of the path for the page not just the page name, such as: site/pagename.jsp

Processes scan settings

To create a custom scan for a specific process, enter the information shown in the table below into the custom scan window after selecting the Processes scan type.

Scan Parameter	Description
Label	This label appears in the Results page information to identify which scan the host failed.
Web Address	The URL of the page with information regarding this process. If entered, this link appears on the Results page. This is a user created web page. It must be stored in: /bsc/Registration/registration/site When completing this field you must enter part of the path for the page not just the page name, such as: site/pagename.jsp
Severity	The severity of the failure if the process is not running on the host. If you select Required and the process does not exist, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See Severity level on page 569 for more details.

Scan Parameter	Description
Process Name	The name of the process being scanned for on the host. This name is seen when you use ps at the command line. This is not necessarily the name in the Activity Monitor list. For example, iChat, iChatAgent, iTunes, iTunesHelper.

Prohibited processes scan settings

To create a custom scan for a specific prohibited process, enter the information shown in the table below into the custom scan window after selecting the Prohibited Processes scan type.

Scan Parameter	Description
Label	This label appears in the Results page information to identify which scan the host failed.
Web Address	The URL of the page with information regarding this prohibited process. If entered, this link appears on the Results page. This is a user created web page. It must be stored in: <code>/bsc/Registration/registration/site</code> When completing this field you must enter part of the path for the page not just the page name, such as: <code>site/pagename.jsp</code>
Severity	The severity of the failure if the prohibited process is running on the host. If you select Required and the prohibited process does exist, the host fails the custom scan. If you select Warning, the host pass the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See Severity level on page 569 for more details.
Process Name	Name of the prohibited process being scanned for on the host.

Linux

The custom scans feature allows you to search host computers for very specific information. Custom scans must be created separately for different operating systems. Within each operating system, there are different types of scans that can be created. Refer to **Add A Linux Scan** below for a list of scan types and general instructions on adding scans. Refer to the instructions for each scan type for field level information. You can modify or remove the scans at any time. When a custom scan is modified it affects any existing general scans that use that custom scan.

Add a custom scan

1. Click **Policy & Objects**.
2. Expand **Endpoint Compliance**.
3. Click the **Scans** option to select it.
4. At the bottom of the window, click **Custom Scans**.
5. Select **Add**.
6. Select **Linux** from the **Operating System** drop-down list.
7. Select the type of scan desired. Each scan type has a special set of fields that are specific to that type. Use the table below for settings.

Scan Type	Description
File	Test for the existence of a specific file on the host. See File scan settings on page 566 .
Package	Test for a existence of a specific rpm/deb packages on the host. See Package scan settings on page 567 .
Processes	Test for the existence of a specific process. See Processes scan settings on page 567 .
Prohibited-Processes	Test for the existence of a specific prohibited process. See Prohibited processes scan settings on page 568 .
Script	Allows users to upload a script to FortiNAC to be executed on the host. See Script settings on page 568 .

8. Enter the **Name** for the custom scan.
9. Enter the information for the custom scan.
10. Click **OK**.

The name of the custom scan will now appear in the **Custom Scans** section for each Linux scan and can be selected as part of the creation or modification of the general scan parameters.

File scan settings

To create a custom scan for a specific file, enter the information shown in the table below into the custom scan window after selecting the File scan type.

Scan Parameter	Description
Label	This label appears in the Results page information to identify which scan the host failed.
Severity	The severity of the failure if the file is not on the host. If you select Required and the file does not exist, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See Severity level on page 569 for more details.
File Name	The name of the file being checked for on the host.
Starting Path	The search for the file starts with the directory indicated here and includes all sub-directories and files. Important: Use the forward slash (/) to delimit directory names. Do NOT use a colon (:).
Web Address	The URL of the page with information regarding this file. If entered, this link appears on the Results page. This is a user created web page. It must be stored in: <code>/bsc/Registration/registration/site</code> When completing this field you must enter part of the path for the page not just the page name, such as: <code>site/pagename.jsp</code>

Scan Parameter	Description
Prohibit this product	If the file is found and this is set to true, the host fails the scan for a prohibited product. Default = false.

Package scan settings

To create a custom scan for a specific rpm or deb package, enter the information shown in the table below into the custom scan window after selecting the Package scan type.

Use this custom scan to check whether particular updates or patches have been applied to the host.

Scan Parameter	Description
Label	This label appears in the Results page information to identify which scan the host failed.
Severity	The severity of the failure if the package is not on the host. If you select Required and the package does not exist, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See Severity level on page 569 for more details.
Package Name	The name of the rpm or deb package being searched for on the host. The custom scan runs rpm or dpkg commands to search for installed packages.
Version	The inclusive minimum version of the Linux software.
Web Address	The URL of the page with information regarding this rpm or deb package. If entered, this link appears on the Results page. This is a user created web page. It must be stored in: <code>/bsc/Registration/registration/site</code> When completing this field you must enter part of the path for the page not just the page name, such as: <code>site/pagename.jsp</code>

Processes scan settings

To create a custom scan for a specific process, enter the information shown in the table below into the custom scan window after selecting the Processes scan type.

Scan Parameter	Description
Label	This label appears in the Results page information to identify which scan the host failed.
Web Address	The URL of the page with information regarding this process. If entered, this link appears on the Results page. This is a user created web page. It must be stored in: <code>/bsc/Registration/registration/site</code> When completing this field you must enter part of the path for the page not just the page name, such as: <code>site/pagename.jsp</code>

Scan Parameter	Description
Severity	The severity of the failure if the process is not running on the host. If you select Required and the process does not exist, the host fails the custom scan. If you select Warning, the host passes the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See Severity level on page 569 for more details.
Process Name	The name of the process being scanned for on the host. This name is seen when you use ps at the command line.

Prohibited processes scan settings

To create a custom scan for a specific prohibited process, enter the information shown in the table below into the custom scan window after selecting the Prohibited Processes scan type.

Scan Parameter	Description
Label	This label appears in the Results page information to identify which scan the host failed.
Web Address	The URL of the page with information regarding this prohibited process. If entered, this link appears on the Results page. This is a user created web page. It must be stored in: <code>/bsc/Registration/registration/site</code> When completing this field you must enter part of the path for the page not just the page name, such as: <code>site/pagename.jsp</code>
Severity	The severity of the failure if the prohibited process is running on the host. If you select Required and the prohibited process does exist, the host fails the custom scan. If you select Warning, the host pass the custom scan and a Policy Warning event is generated. This event can be mapped to an alarm and set to notify the Administrator. See Severity level on page 569 for more details.
Process Name	Name of the prohibited process being scanned for on the host.

Script settings

To create a custom scan for a specific script, enter the information shown in the table below into the custom scan window after selecting the Script scan type.

Scan Parameter	Description
Label	This label appears in the Results page information to identify which scan the host failed.
Upload Script	Users can select a script to upload to FortiNAC. The name of the uploaded script appears in the text field.
Return Value	The value that the script must return after the agent executes the script.
Web Address	The URL of the page with information regarding this prohibited process. If entered, this link appears on the Results page. This is a user created web page. It must be stored in:

Scan Parameter	Description
	<pre>/bsc/Registration/registration/site</pre> When completing this field you must enter part of the path for the page not just the page name, such as: <pre>site/pagename.jsp</pre>

Severity level

You can configure custom scans with a Severity Level setting. The Severity Level controls whether a host loses access to the network or only receives a warning when it is not in compliance with the scan. When the host fails a custom scan with a severity level set to warning, the experience varies, depending on the type of security agent that is being used.

Required

When a custom scan severity level is set to **Required**, if the host fails the scan, the host is set to **At Risk**. The browser is redirected to a web page that contains details about the requirements the host failed. The host self-remediates (corrects the issues causing the failure) and rescans until it meets all requirements. When the host passes the requirements, it is moved to the production network.

The **Scan Results** section of the **Health** tab on the **Host Properties** window shows a **Failed** or **Passed** result. See [Host health and scanning on page 224](#).

Warning

When the host fails a custom scan with a severity level set to **Warning**, the experience will vary depending on the type of security agent that is being used.

Dissolvable Agent

When a host fails the scan, the browser is redirected to a web page that contains details about the requirements the host failed. The web page is divided into two sections. One section contains required severity level items the host failed; the other contains warning severity level items the host failed.

If the host failed only warning severity level items, a **Register Now** button is available on the web page. The user clicks the button and is moved to the Success web page.

If the host failed required and warning severity level items, the host must self-remediate until all items in the Required section are corrected. When only Warning level items are listed in the Warning section of the web page, the **Register Now** button becomes available. The user clicks the button and is moved to the Success web page. The host is not fully compliant with the endpoint compliance policy, but is allowed on the production network.

Persistent Agent

If the host fails the scan for only items with the severity level set to warning, a **Warning** message is sent to the host and the host is moved to the production network.

If the host fails items with severity levels set to Required and Warning, the host is moved to the remediation network. The browser is redirected to a web page containing details about the requirements the host failed. The web page is divided into two sections. One section contains Required severity level items the host failed; the other contains Warning severity level items the host failed.

The host must self-remediate until all items in the Required section are corrected. When the only items listed are in the section containing the failures for severity level set to Warning, the user receives a warning message that his computer is not fully compliant with the endpoint compliance policy. The host is then allowed on the production network.

Configure the Warning message in **System > Settings > Persistent Agent > Properties**. See [Properties on page 919](#).

The **Scan Results** section of the **Health** tab on the **Host Properties** window shows a warning result. See [Host health and scanning on page 224](#).

Use case

The company network rules prohibit registered hosts on the network from having LimeWire installed on the host. Hosts are required to have a Persistent Agent and are scanned daily to maintain compliance. If LimeWire is installed, the host will receive three warnings before being removed from the network.

To set up a custom scan to enforce this rule:

1. Create a custom scan for registry key, enter the details for LimeWire, set **Prohibit** to **True**, and set the **Severity Level** to **Warning**. See [Windows Custom Scan on page 570](#) or [macOS on page 562](#).
2. Create a regular scan and enable the custom scan within that scan. See [Add or modify a scan on page 547](#).
3. Schedule the regular scan to be rerun daily. See [Schedule a scan on page 556](#).
4. Create an endpoint compliance policy that contains the regular Scan. See [Policies on page 531](#).
5. Map the Security Risk Host event to an alarm that will take action on the third occurrence of the event, and set the host At Risk and Send a message. See [Add or modify alarm mapping on page 787](#).
6. Configure the **Persistent Agent Properties Warning** message block. See [Properties on page 919](#).
7. Configure the web page that the host will be redirected to when moved to Remediation. The web page used is created outside the program. In order to keep this page from being overwritten during an upgrade, it should be stored in `/bsc/Registration/registration/site`. Then, return to your custom scan and modify it to contain the new web address.

If the host fails the scan, the first two times, the Warning message is sent. On the third failure, the host is sent the Warning message, is marked At Risk, and moved to Remediation. The web page informs the user about the failure to meet policy requirements. The host self-remediates and rescans. When the host passes the policy, the host is moved back to the production network.

Windows Custom Scan

The custom scans feature allows you to search host computers for very specific information. Custom scans must be created separately for different operating systems. Within each operating system, there are different types of scans that can be created. Refer to **Add A Windows Custom Scan** below for a list of scan types and general instructions on adding scans. Refer to the instructions for each scan type for field level information. You can modify or delete the scans at any time. When a scan is modified, it affects any existing scan that use that custom scan.

Add a custom scan

1. Click **Policy & Objects**.
2. Expand **Endpoint Compliance**.
3. Click the **Scans** option to select it.
4. Click **Custom Scans**.

5. Select **Add**.
6. Select **Windows** from the **Operating System** drop-down list.
7. Select the type of scan desired. Each scan type has a special set of fields that are specific to that type. Use the table below for settings.

Type	Description
Cert-Check	Custom Scan Template used for verifying a valid certificate on the host. Requires Agent Version 3.5 or higher.
Domain-Check	Custom Scan Template used for verifying the domain joined by the host. Scan is not Windows OS specific (Windows XP, Windows 7, etc).
File	Custom Scan Template used for verifying the existence and version of a specific file. If the file exists and is an executable the program can be forced to run.
HotFixes	Custom Scan Template used for verifying the existence of specific HotFixes for the specified Operating systems.
Process-Check	Custom Scan Template used for verifying a required process or check for a prohibited process.
Registry-Keys	Custom Scan Template used for verifying a specific registry key and its associated data.
Registry-Version	Custom Scan Template used for verifying a specific program and its version. The program can be required for specific versions of Windows.
Service	Custom Scan Template used for verifying the state of a service running on the operating system. Requires Agent Version 3.5 or higher.

8. Enter the **Name** for the custom scan.
9. Enter the information for the custom scan.
10. Click **OK**.
11. The name of the custom scan displays in the **Custom Scans** section for each scan. You can select the custom scan to be part of the creation or modification of scan parameters.

List of Deprecated Scans

The following are deprecated scans.

Deprecated Scans	Descriptions
Processes	Custom Scan Template used for verifying the existence of a specific process name for the indicated Windows operating system. Note: This custom scan template has been replaced by "Process-Check".
Prohibited-Processes	Custom Scan Template used for verifying the existence of a specific prohibited process for the indicated Windows operating system(s). Note: This custom scan template has been replaced by "Process-Check".
Domain-Verification	Custom Scan Template used for verifying the domain joined by the host. Note: This custom scan template has been replaced by "Domain-Check".

Deprecated Scans	Descriptions
Prohibited - Domain-Verification	Custom Scan Template used for verifying the domain joined by the host. Requires Agent Version 2.2.2 or higher. Using a lower version of the agent causes all hosts to pass the scan regardless of the domain returned. Note: This custom scan template has been replaced by "Domain-Check".

Certificate check

The certificate being scanned must be obtained from the CA (e.g., Windows AD server), and installed on the host in the certificate Store under **Local Computer > Personal > Certificates**. The certificate must then be uploaded to FortiNAC's certificate management to the Persistent Agent cert-check target. Go to **System > Settings** and under **Security** click **Certificate Management**. Click **Upload Certificate**, and then select the **Persistent Agent Cert Check** target.

Requirements for client certificates:

- The certificate must be signed by a CA specified by the customer.
- Host must be joined to a Windows domain.
- The certificate selected by the agent should adhere to the uses as specified:
- The certificate is a client certificate that is located in the certificate Store on the host under **Local Computer > Personal > Certificates**.
- The host name can be found in the certificate as part of the certificate's subject alternative name (SAN). For example, DNS Name=Win7QA.qatest.com.
- The agent must also be able to sign data using the certificate's private key, so the key usage must have "Digital Signature". This refers to the key usage, not the enhanced key usage.
- The certificate uploaded to FortiNAC's 'Persistent Agent Cert Check' target must be the CA certificate from the signer of the workstation authentication certificate.



In order to complete and pass this scan, Server and endpoint clocks must be within 5 minutes. If scans are not passing, please verify both clocks are in sync with each other.

To create a custom scan for a certificate check, enter the information shown in the table below into the custom scan window after selecting the certificate check scan type.

Scan parameter	Description
Label (required)	This label appears in the results page information to identify which scan the host failed.
Web Address (optional)	The URL of the page with information about this cert-check. If entered, this link appears on the results page. This is a user created web page. It must be stored in: <code>/bsc/Registration/registration/site</code> When completing this field you must enter part of the path for the page not just the page name, such as: <code>site/pagename.jsp</code>

Scan parameter	Description
Severity (required)	The severity of the failure if the certificate is not on the host. See Severity level on page 569 for more details.
CRL Revocation Checking (optional)	If enabled, CRL revocation checking ensures the certificate has not been revoked by the CA. If the certificate is revoked, the host fails the custom scan. The application server must have access to the web server. When CRL verification is enabled, the server reads the CRL distribution point URIs from the client certificate. The application server will directly download a CRL from an "http://" URI, or indirectly download a CRL from a "ldap://" URI through your configured LDAP servers.
Extended Key Usage Restrictions (optional)	If enabled, determines how the private key may be used. Multiple extensions must be comma-separated. For example, if you select this option and enter "1.3.6.1.5.5.7.3.2, 1.3.6.1.5.5.7.3.1" as the specified extensions, • Disabled - There are no restrictions on key usage extensions. • All of - The certificate must include all of the specified extensions. • Exactly - The certificate must include only the specified extensions. • One or More of - The certificate must have at least one of the specified extensions. • None of - The certificate may have extensions, but it must not have one of the specified extensions.

File scan

To create a custom scan for a specific file, enter the information shown in the table below into the custom scan window after selecting the File scan type.

Scan parameter	Description
Label	This label appears in the results page information to identify which scan the host failed.
Severity	The severity of the failure if the file is not on the host. See Severity level on page 569 for more details.
File Name	The name of the file being checked.
File Contains String	Enter the content that must be present within the file in order for the host to pass the scan (e.g., the version number of a product in a configuration file). When the information is found, the host passes the scan. If the information is not found, the host fails the scan. Requires Agent 4.0.4 or greater.
Registry Key	To speed up the search for a file you can first check the registry to determine the folder in which the file is installed. In this field you would enter the section of the registry where the information about the file you seek resides. For example, if you want to make sure that Windows Messenger is installed on the host, the scan needs to look for msmsgs.exe. Enter the registry key that points to the Value Name containing the location of msmsgs.exe, such as: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MessengerService

Scan parameter	Description
Registry Value Name	The Value Name that contains the path to the file the custom scan is seeking. To continue the example above, the Registry Key listed in the previous field tells the custom scan the part of the registry to access to determine where msmsgs.exe is installed. Once the custom scan is looking in the correct section, it needs to know the specific "container" or Value Name in the registry that has the path to msmsgs.exe, such as: InstallationDirectory The custom scan can begin its search in the directory specified in the "InstallationDirectory" Value Name, such as: "C:\Program Files\Messenger"
Execute	Default = No. Select Yes to run the file when it is located.
Command-Line Options	Command line options to be used when executing the file.
Wait for Execution to Complete Before Continuing	Default = No. If set to Yes, the scan waits until the execution of the program is complete before continuing.
File Version (>=)	The version number of the file has to be greater than or equal to the version number entered here.
Web Address	The URL of the page with information about this file. If entered, this link appears on the Results page. This is a user created web page. It must be stored in: /bsc/Registration/registration/site When completing this field you must enter part of the path for the page not just the page name, such as: site/pagename.jsp
Windows OS	Select the check box next to the version(s) of Windows for which this key is required.
Prohibit this product	If the file is found and this is set to true, the host fails the scan for a prohibited product. Default = false.

Registry key scan

To create a custom scan for a specific registry key, enter the information shown in the table below into the custom scan window after selecting the registry keys scan type.

Scan parameter	Description
Label	This label appears in the results page information to identify which scan the host failed.
Web Address	The URL of the page with information about this registry key. If entered, this link appears on the results page. This is a user created web page. It must be stored in: /bsc/Registration/registration/site When completing this field you must enter part of the path for the page not just the page name, such as: site/pagename.jsp

Scan parameter	Description
Severity	The severity of the failure if the key is not on the host. See Severity level on page 569 for more details.
Hive	The name of the hive to be searched. Supported hives are: • HKEY_CLASSES_ROOT • HKEY_CURRENT_USER • HKEY_LOCAL_MACHINE • HKEY_USERS • HKEY_CURRENT_CONFIG Scanning for registry keys in the HKEY_CURRENT_USER hive will not be successful because the user running Persistent Agent differs from the user logged on to the host.
Key Name	Name of the Registry Key that contains the value being located.
Value Name	The Value Name to be located.
Type	• REG_SZ • REG_DWORD You must enter the REG_DWORD setting as a decimal value, not hexadecimal.
Data	The data to be contained in the selected type.
Action	Select an action from the drop-down list: • Match Value Exactly: The Value Name is used as a path to find the specified Key Name in the tree. Data listed in the scan is compared to the data on the key. If the value and data in the key are exact matches to the specified entries, the scan passes. Otherwise, it fails. • Search keys and values: The Key Name is used as a starting point. The search is for whatever is contained in Data. The data must be found in a key name, a Value name, or the data of all sub-keys of the key entered. • Value contains Data: The Value Name is used as a path to find the specified Key Name in the tree. Data listed in the scan is compared to the data in the value. If the contents in the value contains the data, the scan passes. Otherwise, it fails. • Key has a value: The Value Name is used as a path to find the specified Key Name in the tree. If the key is found by using the name in the value and the data is not empty, the scan passes. Otherwise, it fails. • Sets the value (Use Caution): When checked, this scan ALWAYS PASSES. The scan checks to see if the key exists in the registry key. If it does, the scan overwrites the key to have the specified data. If it does not exist, the scan creates the key and sets the data as specified. When the Type is REG_DWORD, the only actions available are Match Value and Sets the value (Use Caution). Example: Hive Name HKEY_LOCAL_MACHINE Key Name SOFTWARE\Widgets\Setup Value Name Version

Scan parameter	Description
	Data 1.0
DWORD Comparison Operation	This field is enabled only when Type is set to REG_DWORD and Action is set to Match Value. The operator selected here is used in the comparison of the value in the Data field to the Data value in the registry. For example, if this field is set to = then both values must match exactly. If the operator is set to >= the Data value in the host registry must be greater than or equal to the Data value in the custom scan.
Prohibit	If the Registry Key is found and this is set to True, the host fails the scan for a prohibited product. Default = False.
Require for Windows...	Select the check box next to the version(s) of Windows OS for which this key is required. You must select the OS within the custom scan to apply the scan to hosts with the selected OS. If you do not select an OS in the custom scan and the host has that OS, the host automatically passes the general scan.

Hotfixes scan

You can create a custom scan for a specific HotFix. Enter the information shown in the table below into the custom scan window after selecting the HotFix scan type.

As a best practice, add HotFix custom scans to a particular operating system within a general scan. If you enable the HotFix custom scan at the Scan level, every host that is evaluated by the scan is also scanned for the HotFix. Since HotFixes are operating system specific you could inadvertently deny access to the network to many hosts.

Scan parameter	Description
Label	Label in the results page information identifying which scan the host failed.
Web Address	The URL of the page with information about this HotFix. If entered, this link appears on the results page. This is a user created web page. It must be stored in: <code>/bsc/Registration/registration/site</code> When completing this field you must enter part of the path for the page not just the page name, such as: <code>site/pagename.jsp</code>
Severity	The severity of the failure if the HotFix is not on the host. See Severity level on page 569 for more details.
HotFix ID	The name of the HotFix, such as KB123456.
Bypass Service Pack (>=)	Select the Bypass Service Pack check box to display a text field. Enter the numeric value for the Service Pack level in this field. The host must have the specified hotfix (HotFix ID above) OR a service pack level equal to or greater than the set value to pass the scan.
Require for Windows...	Select the check box next to the version(s) of Windows for which this key is required.

Registry version scan

Create a custom scan to verify that a specific version of an application, such as Internet Explorer, is installed on the host. Enter the information shown in the table below into the custom scan window after selecting the Registry-Version scan type. When the scan runs, the registry is checked to see if the installed application has the required version.

Scan parameter	Description
Label	This label appears in the results page information to identify which scan the host failed.
Web Address	The URL of the page with information about this registry version. If entered, this link appears on the results page. This is a user created web page. It must be stored in: <code>/bsc/Registration/registration/site</code> When completing this field you must enter part of the path for the page not just the page name, such as: <code>site/pagename.jsp</code>
Severity	The severity of the failure if the file is not on the host. See Severity level on page 569 for more details.
Hive	The name of the Hive to be searched. Supported hives are: • HKEY_CLASSES_ROOT • HKEY_CURRENT_USER • HKEY_LOCAL_MACHINE • HKEY_USERS • HKEY_CURRENT_CONFIG
Key Name	Name of the Registry Key that contains the value being searched for.
Value Name	The Value Name that must be in the key entry.
Version	The Version that must be in the key entry.
Operation	Select an Operator for the version number: > = >=
Prohibit	If the Registry Key is found and this is set to True, the host fails the scan for a prohibited product. Default = False.
Version Delimiter	The character used to identify the delimiter.
Require for Windows...	Select the check box next to the version(s) of Windows for which this key is required.

Registry date scan

Create a custom scan to compare registry date value. Enter the information shown in the table below into the custom scan window after selecting the Service scan type.

Scan parameter	Description
Label	This label appears in the results page information to identify which scan the host failed.
Web Address	The URL of the page with information about this file. If entered, this link appears on the Results page. This is a user created web page. It must be stored in: <code>/bsc/Registration/registration/site</code> When completing this field you must enter part of the path for the page not just the page name, such as: <code>site/pagename.jsp</code>
Severity	The severity of the failure if the file is not on the host. See Severity level for more details.
Hive	The name of the hive to be searched. Supported hives are: · HKEY_CLASSES_ROOT · HKEY_CURRENT_USER · HKEY_LOCAL_MACHINE · HKEY_USERS · HKEY_CURRENT_CONFIG Scanning for registry keys in the HKEY_CURRENT_USER hive will not be successful because the user running Persistent Agent differs from the user logged on to the host.
Key Name	Name of the Registry Key that contains the value being searched for.
Value Name	The Value Name that contains the date you are trying to compare. The date formats that are supported but not limited to (Time is optional): · yyyy-mm-dd hh:mm:ss · yyyy/mm/dd hh/mm/ss · yyyy-mm-ddThh:mm:ss · yyyy-mm-dd · yyyy/mm/dd · yyyymmdd
Time Unit	The time unit you wish to compare with the date contained in the registry key: · Day · Hour · Minute
Time Interval Before Current	The time before the current time you wish to compare with date in the registry key

Scan parameter	Description
Time Comparison Operation	The comparison operation you wish to use: · >= · > · = · < · <=
Prohibit this product	If the file is found and this is set to true, the host fails the scan for a prohibited product. Default = false.

Processes-Check scan

Create a custom scan for a specific process. Process names for various applications may differ between operating systems. Enter the process name for each OS if this is the case. Enter the process name(s) information into the custom scan window for processes.

If you do not want to scan for a process on a particular operating system, leave the corresponding field blank.

Scan parameter	Description
Label	This label appears in the results page information to identify which scan the host failed.
Web Address	The URL of the page with information regarding this process. If entered, this link appears on the results page. This is a user created web page. It must be stored in: <code>/bsc/Registration/registration/site</code> When completing this field you must enter part of the path for the page not just the page name, such as: When completing this field you must enter part of the path for the page not just the page name, such as: <code>site/pagename.jsp</code>
Severity	The severity of the failure if the process is not running on the host. See Severity level on page 569 for more details.
Process Name for ...	Enter the name of the process that is required for the specific operating system(s).
Prohibit This Product	Set true to prohibit a process, and false to require it.

Domain-Check scan

Create a custom scan to verify that a host has joined the appropriate domain when it connected to the network. Domain names may differ between operating systems. Enter a comma separated list of domain names for each OS. Attach this custom scan to any Policies that require domain verification. A host will pass this scan if it is joined with any domain contained in the list for the host's operating system.

Scan parameter	Description
Label	This label appears in the results page information to identify which scan the host failed.
Web Address	The URL of the page with information regarding domain verification. If entered, this link appears on the results page. This is a user created web page. It must be stored in: <code>/bsc/Registration/registration/site</code> When completing this field you must enter part of the path for the page not just the page name, such as: <code>site/pagename.jsp</code>
Severity	The severity of the failure if the host is not part of any of the domains specified. See Severity level on page 569 for more details.
Domain Names for ...	Enter a comma separated list of the NetBIOS domain names that are required or permitted for the specific operating system(s).
Domains are	Set Required to require a domain and Prohibited to prohibit it.

Service scan

You can create a custom scan to check the status of a Windows Service. Enter the information shown in the table below into the custom scan window after selecting the Service scan type.

Scan parameter	Description
Label	This label appears in the results page information to identify which scan the host failed.
Severity	The severity of the failure if the service is not in the desired state on the host. See Severity level on page 569 for more details.
Service Name	The name of the service on the Windows OS. To retrieve the service name, open the Microsoft Management Console Local Services view. See Find the service name on page 580 for information on how to locate the Service Name on your system.
Desired State	Select the the state of the service on the host to be scanned. Select Running to indicate the host must be running the service. Select Stopped to indicate the host must not be running the service.
Web Address	The URL of the page with information about this service. If entered, this link appears on the Results page. This is a user created web page. It must be stored in: <code>/bsc/Registration/registration/site</code> When completing this field you must enter part of the path for the page not just the page name, such as: <code>site/pagename.jsp</code>

Find the service name

1. Open Microsoft Management Console on your system.
2. Navigate to the Local Services view.
3. Right-click the process you want to create the custom scan for, and click **Properties**.
4. Find the service name in the Properties view and enter it in the **Service Name** field of the custom scan.

Scan parameters

Endpoint compliance policies used to scan your hosts for compliance, have many variables for which the host can be scanned. For the antivirus and operating system variables, you can narrow the scan by setting custom parameters. For example, when scanning for a particular operating system you can require that the operating system be at Service Pack 4 or higher.

Any parameter that you modify will no longer be updated by the Auto-Def Updates scheduled task. That task updates the list of antivirus and operating systems for which you can scan. It also modifies parameters associated with each of those items to force hosts to use the most recent definitions for antivirus and to have installed the latest updates to the operating system.

This section provides details about each type of variable and the detailed parameters within that can be set to narrow your scan further.

Antivirus parameters - Windows

The table below provides an alphabetical list all of the possible parameters that can be configured for antivirus software for Windows. Only some of these parameters are used for any given antivirus program.



Check with your vendor for the required format. Formats for dates, version numbers, .dat files, etc. change frequently and vary by product.



Default parameter values are entered and updated automatically by the scheduled Auto-Def Updates. If the values have been manually edited, the Auto-Def Updates will not override those changes.

Settings

Parameter	Description	Typical options
AntiVirus definition Date	The date of the required AntiVirus definition files.	YYYY-MM-DD
AntiVirus Engine	The version number of the required AntiVirus Engine. Select the operator that will apply to the definition value found on the host: greater than, equal to, or both.	** > = >=
Client Security Antimalware Service must be running	Select a setting.	Enabled or disabled

Parameter	Description	Typical options
Client Security State Assessment Service must be running	Select a setting.	Enabled or disabled
Custom Scans	Select the custom scans that you want to implement for the product.	Custom scans
Daily Virus Definition	The version of the required daily definition files. Select the operator that will apply to the definition value found on the host: greater than, equal to, or both.	** > = >=
Definitions Label	Enter the label for the Definitions Web Address.	Text entry
Definitions Web Address	Enter the URL for the web page where the updated definitions for the selected product can be located and downloaded. When a host fails the scan this URL appears in the Failed Policy Results view.	URL
Definitions Version	The version of the required definition files. Select the operator that will apply to the definition value found on the host: greater than, equal to, or both.	** > = >=
Engine Version	The number of the required engine version. Select the operator that will apply to the definition value found on the host: greater than, equal to, or both.	** > = >=
Engine Version Label	Enter the label for the Engine Version Web Address.	Text entry
Engine Version Web Address	Enter the URL for the web page where the updated engine version for the selected product can be located and downloaded. When a host fails the scan this URL appears in the Failed Policy Results view.	URL
Label	Enter a label. This label will appear on the Results panel to identify which scan the host failed.	Text entry
Macro Definition	The date of the required macro definition files. Select the operator that will apply to the definition value found on the host: greater than, equal to, or both.	YYYY-MM-DD > =

Parameter	Description	Typical options
		>=
Main Virus Definition	The version of the required main definition files. Select the operator that will apply to the definition value found on the host: greater than, equal to, or both.	** > = >=
Minimum Engine Version	Minimum engine version required to pass the scan.	**
Operational Label	Enter a label. This label will appear on the Results panel to identify that an operational state did not meet the requirement.	Text entry
Operational Web Address	Enter the URL of the web page that displays information about the product when the host fails the scan because the Client Security State Assessment or Antimalware Service operational state did not meet the requirement.	URL
Operator (applies to all)	The Engine version and definition (Virus and Spyware) values found on the host must be either greater than, equal to, or both than the value(s) entered.	> = >=
Products to Detect	Select which products you wish to include in the scan. All products are selected by default.  Scan results show the group name (label) only, not the specific AV/AS product. The scan will either pass or fail for the group (label).	
Program Version	The version number of the program. Select the operator that will apply to the definition value found on the host: greater than, equal to, or both.	** > = >=
Program Version Label	Enter the label for the Program Version Web Address.	Text entry
Program Version Web Address	Enter the URL for the web page where the required version can be located and downloaded. When a host fails the scan this URL appears in the Failed Policy Results view.	URL
Prohibit this Product	Set this option to true if you want to prohibit the installation of this product. If this product is installed, the scan fails.	true or false

Parameter	Description	Typical options
Protection Updates	The date of the required Protection Updates file. Select the operator that will apply to the definition value found on the host: greater than, equal to, or both.	YYYYMMDD > = >+
Protection Updates Label	Enter the label for the Protection Updates Web Address.	Text entry
Protection Updates Web Address	Enter the URL for the web page where the Production Updates can be located and downloaded. When a host fails the scan this URL appears in the Failed Policy Results view.	URL
Signature Version	The build number or date and build number of the required signature file. Select the operator that will apply to the definition value found on the host: greater than, equal to, or both.	** > = >=
Signature Version Label	Label for the Signature Version Web Address.	Text entry
Signature Version Web Address	Enter the URL for the web page where the required signature version can be located and downloaded. When a host fails the scan this URL appears in the Failed Policy Results view.	URL
Spyware Definition	Number of the required spyware definition file.	**
Version	The number of the required virus definition file. Select the operator that will apply to the definition value found on the host: greater than, equal to, or both.	** > = >=
Version Label	Enter the label for the Version Web Address.	Text entry
Version Web Address	Enter the URL for the web page where the required version can be located and downloaded. When a host fails the scan this URL appears in the Failed Policy Results view.	URL
Virus Definition	Used to identify the virus definition version installed. May be the name of the definition file, the date of the file, a version number, etc. Select the operator that will apply to the definition value found on the host: greater than, equal to, or both.	** > = >=

Parameter	Description	Typical options
Virus Definition VDF Label	The label for the VDF web address.	Text entry
Virus Definition VDF Web Address	The URL for the web page where updated definitions can be located and downloaded. Supply a local or Internet URL. This URL will be displayed on the Failed Policy Results view if the host fails the scan.	URL
Virus Signature	The date of the required virus signature.	YYYY-MM-DD
Web Address	Enter the URL of the web page that displays information about the product if the host fails the scan.	URL
Windows Operating System	Select any or all Windows operating systems required for the selected product.	
Software specific parameters		
Eset-NOD32 Minimum Scanner Version (nod32.exe)	The number of the required scanner version of the file nod32.exe.	**

Antivirus parameters - macOS

The table below provides an alphabetical list all of the possible parameters that can be configured for antivirus software for macOS. Only some of these parameters are used for any given antivirus program.



Check with your vendor for the required format. Formats for dates, version numbers, .dat files, etc. change frequently and vary by product.



Default parameter values are entered and updated automatically by the scheduled Auto-Def Updates. If the values have been manually edited, the Auto-Def Updates will not override those changes.

Settings

Parameter	Description	Typical options
Definitions Label	Enter the label for the Definitions Web Address.	Text entry
Definitions Web Address	Enter the URL for the web page where the updated definitions for the selected product can be located and downloaded. When a host fails the scan this URL appears in the Failed Policy Results view.	URL

Parameter	Description	Typical options
Engine Version Web Address	Enter the URL of the web page where information about the engine version is displayed if the host fails the scan.	URL
Engine Version Label	Enter the label for the Engine Version Web Address.	Text entry
Label	Enter a label. This label appears in the Results page information to identify which scan the host failed.	Text entry
Program Version	The number of the required version. Select the Operator to apply to the definition value found on the host: greater than, equal to, or both.	** > = >=
Program Version Label	Enter the label for the Program Version Web Address.	Text entry
Program Version Web Address	Enter the URL for the web page where the required program version can be located and downloaded. When a host fails the scan this URL appears in the Failed Policy Results view.	URL
Prohibit this Product	Set this option to true if you want to prohibit the installation of this product. If this product is installed, the scan fails.	true or false
Version Label	Enter the label for the Version Web Address.	Text entry
Virus Definition	Used to identify the virus definition version installed. May be the name of the definition file, the date of the file, a version number, etc. Select the operator to apply to the definition value found on the host: greater than, equal to, or both.	** > = >=
Version Web Address	Enter the URL for the web page where information about the version is displayed when the scan is failed. When a host fails the scan this URL appears in the Failed Policy Results view.	URL
Web Address	Enter the URL of the web page where information about the product is displayed in case the scan fails.	URL
Software specific parameters		
Clam Engine Version	The number of the required engine version. Select the Operator to apply to the definition value found on the host: greater than, equal to, or both.	** > = >=

Operating system parameters - Windows

The table below contains an alphabetical list of possible Configuration Parameters that can be used when setting up scans for Windows. A subset of these parameters is available for each version of this operating system.



Default parameter values are entered and updated automatically by the scheduled Auto-Def Updates. If the values have been manually edited, the Auto-Def Updates will not override those changes.

Settings

Parameter	Description
Allowed Editions	Select the allowed editions. Options are Home Basic, Home Premium, Business, Enterprise, Ultimate, and Starter.
Critical / Security Updates Label	The Critical / Security Updates Label that displays on the results page.
Critical / Security Updates Web Address	The URL for the web page where Windows-Server-2008 Critical / Security Updates information can be located and downloaded. Supply a local or Internet URL to display in the Failed Policy Results window if the host fails the scan.
Custom Scans	Any custom scans that have been created are shown.
Disable Bridging	When selected, disables bridging on the host.
Disable Internet Connection Sharing	When selected Internet Connection Sharing is disabled on the host.
Edition Label	Enter a label. This label appears in the Results page information to identify which scan the host failed.
Edition Web Address	The URL for the web page where the specific edition information can be located and downloaded. Supply a local or Internet URL to display in the Failed Policy Results window if the host fails the scan.
Enable Automatic Updates	See the enable automatic updates parameters table below.
Enable Windows Firewall	When selected, the Windows Firewall is enabled.
Force DHCP	Requires write access to the registry if done through the .  Do not enable Force DHCP on policies that will be used for VPN clients. Enabling this setting can cause the host to continuously lose its VPN connection.
Label	Enter a label. This label appears in the Results page information to identify which scan the host failed.

Parameter	Description
	If a Windows Operating System is selected from the Operating Systems List but none of the following are selected: • Require Version/Build Number • Enable Automatic Updates • Require Critical Updates • Detect Network Bridges • Disable Internet Connection Sharing • Require Security Updates • Trigger SCCM Evaluation Scan results may list all the above with a result of "Passed".
Prohibit Home Edition	When selected, prohibits Windows-XP Home Edition.
Require All Critical Updates	When selected, all Critical Updates are required for the host.
Require Critical Updates	When selected, Require Critical Updates must be enabled on the host.
	FortiNAC leverages the Windows Update tool to check for Critical Updates and Security Updates during an operating system scan. The host must be able to connect to the Microsoft Windows Update web site and any other associated sites.
	In the event that the local WSUS server is unreachable, FortiNAC does not revert to using the Microsoft update servers. FortiNAC will not generate events when a host fails to contact the WSUS server because it occurs on the endpoints and not on FortiNAC. However, a local event log entry is created for hosts that fail to connect to the WSUS server.
Require Security Updates	When selected will Require Security Updates to be enabled on the host.
Require Service Pack	When the checkbox labeled "Require Service Pack" is selected a text field displays. Enter the numeric value for the Service Pack Level.
SCCM Evaluation Label	The SCCM Evaluation label that is displayed in scan results to indicate that the SCCM Evaluation was triggered for the host.
Service Pack Label	The Service Pack Label that displays on the results page.
Service Pack Level	The required Service Pack Level. Enter the numeric value. Select the Operator to apply to the definition value found on the host: greater than, equal to, or both.
Service Pack Web Address	URL for the web page where Service Pack information can be located and downloaded. Supply either a local or Internet URL. This URL is displayed in the Failed Policy Results window if the host fails the scan.
Trigger SCCM Evaluation	When selected, an upgrade is forced on the host from the SCCM controller. This ensures all hosts on the network are up-to-date. No error is generated within FortiNAC. See the SCCM controller for failure details.

Parameter	Description
	 This option is available for Windows 7, 8, 10, Windows-Server-2012, Windows-Server-2008-R2, and Windows-Server-2012-R2.
Edition Label	The Updates Label that displays on the results page.
Validate Edition	When enabled, only those editions of Windows that are selected in FortiNAC are permitted. When disabled, all/any edition of the selected Windows operating systems will be allowed, such as Windows Vista N or Windows Vista K.
Web Address	The URL for the web page where Windows operating system information can be located and downloaded. Supply either a local or Internet URL. This URL is displayed in the Failed Policy Results window if the host fails the scan.

Enable automatic updates parameters

When this option is checked for the selected operating system, it enables Automatic Updates on the host by modifying the registry. Additional configuration options appear once the box is selected. Use CAUTION when changing any of the Auto Update Settings. It is recommended that you are familiar with these options before you make any changes.

Parameter	Description
Auto Update Web Address	Web address used for Windows update. The default is sma/windowsupdates.jsp.
Apply as a Policy (users can't modify)	Select True or False. Default = True. If this option is enabled, users of hosts running the selected version of Windows can no longer set Windows Update Parameters for their own hosts. Registry keys for those settings are set by FortiNAC and are locked. Changing this option to False does not remove the lock from the registry keys. The keys must be deleted to restore user access to Windows Update settings. Keys are as follows: <pre>SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU</pre>
RescheduleWaitTime	Time to wait between the time Automatic Updates starts and the time it begins installations, where the scheduled times have passed. The time is set in minutes from 1 to 60, representing 1 minute to 60 minutes).  This setting only affects host behavior after the hosts have updated to the SUS SP1 client version or later.
NoAuto RebootWithLoggedOnUsers	Select True or False. Default = False. If set to true, Automatic Updates does not automatically restart a computer while users are logged on. This setting affects host behavior after the hosts have updated to the SUS SP1 host version or later.
NoAutoUpdate	0 = Automatic Updates is enabled. 1 = Automatic Updates is disabled.

Parameter	Description
	Default = 0
AUOptions	1 = Keep my computer up to date has been disabled in Automatic Updates. 2 = Notify of download and installation. 3 = Automatically download and notify of installation. 4 = Automatically download and schedule installation.
AUState	0 = Initial 24-hour timeout (Automatic Updates doesn't run until 24 hours after it first detects an Internet connection.) 1 = Waiting for the user to run Automatic Updates 2 = Detection pending 3 = Download pending (Automatic Updates is waiting for the user to accept the pre-downloaded prompt.) 4 = Download in progress 5 = Install pending 6 = Install complete 7 = Disabled 8 = Reboot pending (Updates that require a reboot were installed, but the reboot was declined. Automatic Updates will not do anything until this value is cleared and a reboot occurs.)
ScheduledInstallDay	0 = Every day. 1 - 7 = The days of the week from Sunday (1) to Saturday (7).
ScheduledInstallTime	The time of day in a 24-hour format (0-23).
UseWUServer	Select True or False Use or not use a server that is running Software Update Services instead of Windows Update.
WUServer	http://<server> This value sets the SUS server by HTTP name (for example, http://IntranetSUS).
WUStatusServer	http://<server> This value sets the SUS statistics server by HTTP name (for example, http://IntranetSUS).



If you configure the scan to enable Automatic Updates and an error occurs (for example, a network or permission error) so that the scan cannot perform the update, then the scan might fail.

Operating systems parameters - macOS

The table below contains an alphabetical list of possible Configuration Parameters for macOS. A subset of these parameters is available for each operating system.



Default parameter values are entered and updated automatically by the scheduled Auto-Def Updates. If the values have been manually edited, the Auto-Def Updates will not override those changes.

Settings

Parameter	Description	Typical options
Label	Enter a label. This label appears in the Results page information to identify which scan the host failed.	Text entry
Web Address	The URL for the web page where Mac information can be located and downloaded. Supply a URL to display in the Failed Policy Results window if the host fails the scan.	URL
Label for Update Version	Enter a label.	Text entry
Update Version Web Address	The URL for the web page where Mac update information can be located and downloaded. Supply either a local or Internet URL.	URL
Require at least Version 10.x.	Numerical entry for x in the version 10.1.x	Number
Custom Scans	Any custom scans that have been created will be shown.	Select a custom scan.

Actions

The **Actions** view allows you to add, modify, and delete actions that can be associated to an alarm. If the action is selected, it can be executed automatically or manually, depending on the security rule configuration.

Settings

Field	Definition
Add Filter	Allows you to select a field from the current view to filter information. Select the field from the drop-down list, and then enter the information you wish to filter. See Filters on page 34 .
Update	Displays the filtered data in the table.
Table columns	
Name	User defined name for the action. The type of action that will occur if the rule is enabled.
Activity Failure	Indicates whether the system will continue to perform activities for the action if a higher-ranked activity fails. When Continue Running Activities is selected, the next ranked activity in the list is performed after a higher-ranked activity fails. When Stop Running Activities is selected, no lower-ranked activities are executed when a higher-ranked activity fails.

Field	Definition
Secondary Task Delay	The amount of time that will pass before the enabled secondary activity is executed for an activity. For example, the user may wish to enable the host 15 minutes after the host was initially disabled.
Activity Summary	A description of the activity that will occur.
Last Modified By	User name of the last user to modify the action.
Last Modified Date	Date and time of the last modification to this action.
Right click options	
Delete	Deletes the selected action.
Modify	Opens the Modify Security Action window for the selected action.
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746 .
 You must have permission to view the admin auditing log. See Add an administrator profile on page 139.	

Add or modify an action

1. Go to **Logs > Security Incidents > Actions**
2. Click **Add** or select an existing security action and click **Modify**.
3. Click in the **Name** field and enter a name for this security action.
4. Use the table below to enter the security action information.
5. Click **OK** to save your security rule action.

Settings

Field	Definition
Name	A name for this security action.
On Activity Failure	User indicates whether the system will continue to perform activities for the action if a higher- ranked activity fails. When Continue Running Activities is selected, the next ranked activity in the list is performed after a higher-ranked activity fails. When Stop Running Activities is selected, no lower-ranked activities are executed when a higher-ranked activity fails.
Perform Secondary Tasks After check box	When selected, if a secondary task is enabled for an activity, the secondary task is automatically executed to undo the action. The user may enter the amount of time that will pass between the primary and secondary tasks. If the check box is not selected, the user may manually undo the action in the Security Alarms view.

Field	Definition
Not currently in use/In use by	Indicates whether the action is in use, and the number of rules currently associated with the action.
Activities	
Rank Buttons	Moves the selected action up or down in the list. Activities are performed in order by rank.
Rank	The activity's rank in the list of activities. Rank controls the order in which activities are performed.
Activity	Specifies the activity that will be performed.
Add	Click to add an activity.
Modify	Click to modify a selected activity.
Delete	Click to delete a selected activity.

Delete an action

1. Select **Logs > Security Incidents > Actions**
2. Select an action and click **Delete**.
3. A confirmation message is displayed. Click **Yes** to continue.

Add or modify activities

1. Select **Logs > Security Incidents > Actions**
2. Click **Add** or select an action and click **Modify**.
3. Under **Activities**, click **Add**, or select an activity and click **Modify**.
4. Select the activity from the **Activity** drop-down menu.
5. Enter the information associated with the activity.
6. Some options include the **Secondary Task** check box. Selecting this check box enables the secondary task to occur after the time period specified in the action has passed.
7. Use the table below for information about each activity option.
8. Click **OK** to save your activity.

Settings

Field	Definition
Command Line Script Action	Lets you specify a particular command line script to be executed as an alarm action.
Send Alarm to Custom Script	Lets you send an alarm to a custom command line script located in /home/cm/scripts when the trigger event occurs.

Field	Definition
Send Alarm to External Log Hosts	Sends an alarm to an external log host when the trigger event occurs.
Email User Action	Sends an email to the logged on user or owner, only the logged on user, or only the owner when the action is taken. See Hosts on page 213 for more information about adding or modifying the host's owner. Enter the message for the user in the Email Message box. Select the fields to display information you wish to append to the email. You can update the text to be displayed for each field. Users can add or modify custom fields that are appended to the email. Custom fields include information about a security event that is stored under Full Event Attributes in the Security Events View > Event Details window. For example, enter a label for the field and the "CS4" key to display the CS4 information in the custom field. See Events on page 814
Email Group Action	Sends an email to the selected administrator group.
SMS User Action	Sends an SMS message to the host's owner when the action is taken. See Hosts on page 213 for more information about adding or modifying the host's owner. Enter the message for the user in the SMS Message box.
Host Role Action	Lets you set the host role to any configured role. You can select the Secondary Task check box to enable a secondary task to change the role when the action is undone.
Disable Host	Disconnects the host from the network. You can select the Secondary Task check box to enable the host after a specified time period if the Perform Secondary Task(s) check box is enabled for the action.
Disable Port	Disconnects the port. You can select the Secondary Task check box to enable the port after a specified time period if the Perform Secondary Task(s) check box is enabled for the action.
Run Endpoint Compliance Configuration	When selected, allows you to run additional endpoint compliance configurations based on security actions mapped to a scan's results. See Chaining configuration scans on page 540 .
Mark Host At Risk	Automatically fails the scan selected in the Mark Host At Risk For drop-down list, and places the host in a state of remediation the next time the host connects. You can select the Secondary Task check box to mark the host safe after a specified time period if the Perform Secondary Task(s) check box is enabled for the action.
Mark Host Safe	Automatically marks the host as safe for the scan selected in the Mark Host Safe For drop-down list, and passes the scan. You can select the Secondary Task check box to mark the host at risk after a specified time period if the Perform Secondary Task(s) check box is enabled for the action.
Send Message to Desktop	Lets you send a message to the desktop of a host running the Persistent Agent.

Delete an activity

1. Go to **Logs > Security Incidents > Actions**
2. Select an action and click **Modify**.

3. Select an activity and click **Delete**. The activity is deleted.
4. Click **OK**.

Supplicant EasyConnect

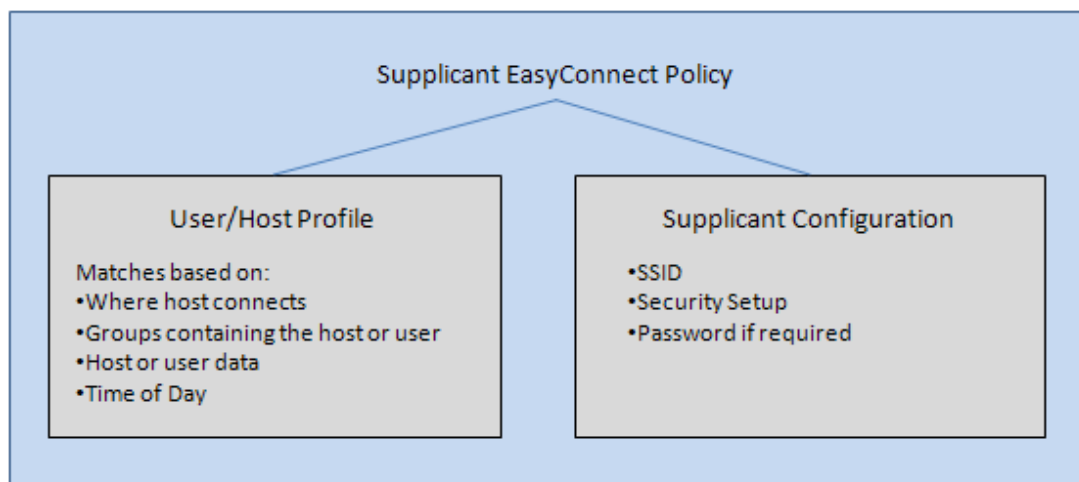
Supplicant EasyConnect policies are used to help your network users connect to the network quickly in a wireless environment. Supplicant policies contain a supplicant configuration and a user/host profile. When a host needs a supplicant, FortiNAC compares the user and host data to the user/host profile in each Supplicant Policy starting with the first policy in the list. When a match is found, the Supplicant Policy is applied to the connecting host and the supplicant configuration is used to setup the supplicant on the host.



There may be more than one Supplicant Policy that is a match for this host/user; however, the first match found is the one that is used.

If you create a user/host profile with fields Where set to Any, Who/What by Group set to Any, Who/What by Attribute set to Any and When set to Always, it matches ALL users and hosts. This is essentially a Catch All profile. If this user/host profile is used in a policy, all policies below that policy are ignored when assigning a policy to a user or a host. To highlight this, policies below the policy with the catch all profile are grayed out and have a line through the data.

The best way to use a Catch All profile is to create a general policy with that profile and place it last in the list of policies.



Supplicant Policies are applied to the host using an agent, except in the case of iOS devices where the user is prompted to download the configuration from the Captive Portal. The Dissolvable Agent or the Persistent Agent is used for Windows and macOS hosts and the Mobile Agent is used for Android devices.

The host connection location does not determine the supplicant configuration applied unless the location is part of the user/host profile. Therefore, a host could connect on an SSID, and actually be configured for a different SSID because the user/host profile matched a Supplicant Policy with a higher rank that contained the configuration for a different SSID.

Host configuration process

The host supplicant configuration setup process is as follows:

1. Host connects to the network.
2. Host connects to an open SSID based on the operating system of the host. If authenticating through LDAP, the user must be in the selected directory group configured in the SSID mapping. You configure SSID mapping with a supplicant configuration.
3. If the user is on a Windows or macOS device, the user downloads either the Persistent Agent or the Dissolvable Agent. The agent applies the Supplicant Configuration after scanning and registering the host.
4. If the user is on an Android device, the user downloads and runs the Mobile Agent. The agent applies the Supplicant Configuration after scanning and registering the host. See [Mobile Agent on page 506](#) for download requirements.
5. FortiNAC compares user and host data to supplicant policies and finds the first match starting from the top of the list of policies.
6. The user registers or authenticates.
7. The supplicant configuration is applied.
8. The Agent attempts to move the host to the SSID that was just configured.

FortiNAC supports the configuration of encrypted networks as follows:

- Open
- WEP (PSK)
- WPA (PSK)
- WPA2 (PSK)
- WEP Enterprise
- WPA Enterprise(PEAP)
- WPA2 Enterprise(PEAP)

WPA Enterprise and WPA2 Enterprise are limited to PEAP-MSCHAPv2.

Requirements

To use Supplicant EasyConnect policies to configure the supplicant on hosts that connect to your wireless network, the following requirements must be met:

- If your RADIUS server is configured with a certificate it must be a trusted third-party certificate from a CA such as Verisign or Thawte. If you have used a self-signed certificate it must be distributed to all hosts or you must replace it with a trusted third-party certificate. FortiNAC will not be able to configure the supplicant unless these certificates are correct.
- You must have at least one Isolation VLAN, such as Registration or Remediation. If you do not, use the Configuration Wizard to configure an Isolation context. See the *Appliance Installation Guide* for instructions on running the Configuration Wizard.
- Supplicant Easy Connect Policies are only supported on the following operating systems:
Having the required Windows Service Packs installed ensures that the host is transitioned to the secure SSID without having to close the browser and reopen:
 - Windows 7 Service Pack 1 and higher
 - Windows 8, 8.1, 10 and higher



Windows 10 hosts using the random hardware address functionality may experience unpredictable and undesired results with the Supplicant Easy Connect feature.

- macOS 10.7 and higher
 - Android 2.3.3 or higher
 - iOS 4.0 or higher
 - Supplicant EasyConnect Configurations can only be applied as follows:
 - For Windows and macOS hosts you must use the Dissolvable Agent or the Persistent Agent
 - For Android devices you must use the Mobile Agent. Mobile Agent requires the use of a certificate from a CA. A self-signed certificate cannot be used. See [SSL certificates on page 509](#).
 - iOS and macOS users need to select the secure SSID because they will not be switched to that SSID automatically after applying the supplicant configuration.
 - Supplicant configurations are applied to the host using an agent, except in the case of iOS devices where the user is prompted to download the configuration from the Captive Portal. The Dissolvable Agent or Persistent Agent are used for Windows and macOS hosts and the Mobile Agent is used for Android devices.
 - Supplicant configurations for Windows hosts connecting on an SSID that uses WEP Enterprise, WPA Enterprise, WPA2 Enterprise for security require that you upload the CA or Root certificate for the valid SSL certificate used to secure the RADIUS server. FortiNAC parses the CA certificate in order to read the CA fingerprint. This allows the supplicant configuration to be applied correctly and to switch the Windows host from the Open SSID to the Secure SSID. CA or Root certificates can be downloaded from the CA that issued your SSL certificate. See [Create or edit a configuration on page 601](#) and [Open SSID for device onboarding on page 82](#).
 - If you would like to modify the text displayed to Apple iOS users in the captive portal, go to the portal content editor and modify **Profile Configuration Download** under the appropriate Isolation context, such as Registration or Remediation. See [Content editor on page 632](#).
 - Configure Isolation VLANs on the Model configuration for the wireless devices being used or the individual SSIDs being used. See [Model configuration on page 338](#) or [SSID configuration on page 367](#).
 - Create an endpoint compliance policy that uses the Dissolvable Agent or the Persistent Agent for Windows and macOS hosts and the Mobile Agent hosts. The user/host profile created for this endpoint compliance policy must have information in it that will match a connecting host that needs to have a supplicant configured. For example, the User/Host profile could have a group of wireless devices as the connection location and Host operating system in the Who/What by Attribute field. See [Policies on page 531](#) and [Agent packages on page 992](#).
-



It is recommended that you modify the associated scan to require Service Pack 1 and higher for Windows 7. Having these Service Packs installed ensures that the host is transitioned to the secure SSID without having to close the browser and reopen.



In some cases, when the supplicant configuration is applied using the Persistent Agent, the host cannot be transitioned to the secure SSID automatically. The user must connect to the SSID manually.

- Create at least one user/host profile that has criteria that matches the hosts who will need a Supplicant, such as operating system or connection location. See [User/host profiles on page 466](#).
 - Create at least one supplicant configuration with the setup parameters for the SSID that hosts will use. See [Supplicant configurations on page 600](#).
 - Create at least one Supplicant EasyConnect Policy that maps the supplicant configuration to a user/host profile. See [Supplicant EasyConnect on page 595](#).
-

Manage policies

Add, modify or delete Supplicant EasyConnect policies used to configure Supplicants on connecting hosts.



If the user/host does not match any policy, no supplicant configuration is provided.

If you create a user/host profile with fields Where set to Any, Who/What by Group set to Any, Who/What by Attribute set to Any and When set to Always, it matches ALL users and hosts. This is essentially a Catch All profile. If this user/host profile is used in a policy, all policies below that policy are ignored when assigning a policy to a user or a host. To highlight this, policies below the policy with the catch all profile are grayed out and have a line through the data.

The best way to use a Catch All profile is to create a general policy with that profile and place it last in the list of policies.

Settings

An empty field in a column indicates that the option has not been set.

Field	Definition
Rank	Policy's rank in the list of policies. Rank controls the order in which host connections are compared to Policies.  Set Rank is now legacy architecture. In 7.2, use drag and drop to reorder the rank from the left column, click edit from within the cell.
Name	User defined name for the policy.
Configuration	Contains the configuration for the SSID, Security Settings and password if required. See Supplicant configurations on page 600 .
Who/What	Attributes User or Host attributes specified in the selected user/host profile. The connecting host or user must have the attributes to be a match. See Filter example on page 468. Do not select user attributes in user/host profiles used to assign a portal. FortiNAC does not have access to any user attributes when an unregistered host connects to the network. Only the following host attributes are known at the time of connection: connection location, IP address, MAC address, and operating system. RADIUS Attributes Indicates whether or not attribute filters have been created for this Profile. RADIUS attribute filters are used to match against endpoints pre- and post-authentication. Groups User or Host group or groups specified in the user/host profile. These groups must contain the connecting user or host for the connection to be a match for this policy. When set to Any, this field is a match for all hosts or users.

Field	Definition
	It is not recommended that you use groups in user/host profiles for Portal assignment because an unregistered host will not be contained in any host groups and user data is unknown until after the portal is assigned.
Where	The connection location specified in the user/host profile. The host must connect to the network on a device, port or SSID contained within one of the groups shown here to be a match. When set to Any, this field is a match for all hosts or users.
When	The time frame specified in the selected user/host profile. The host must be on the network within this time frame to be a match. When set to Always this field is a match for all hosts or users.
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746 .
 You must have permission to view the admin auditing log. See Add an administrator profile on page 139 .	

Create or edit a policy

1. Select **Policy & Objects**.
2. Select **Supplicant EasyConnect**.
3. Click **Create New** or select an existing policy and click **Edit**.
4. Click in the **Name** field and enter a name for this policy.
5. Select a **User/Host Profile** from the drop-down menu. You can use the icons next to the **User/Host Profile** field to add a new profile or modify the profile shown in the drop-down menu. Note that if you modify this profile, it is modified for all features that make use of the profile. Connecting hosts must match this user/host profile to be assigned the supplicant configuration specified in the next step.
6. Select a **Supplicant Configuration** from the drop-down menu. You can use the icons next to the **Supplicant Configuration** field to add a new configuration or modify the configuration shown in the drop-down menu. Note that if you modify this configuration, it is modified for all features that make use of it. See [Create or edit a configuration on page 601](#).
7. The **Note** field is optional.
8. Click **OK** to save your policy.

Delete a policy

1. Click **Policy & Objects**.
2. Select **Supplicant EasyConnect**.
3. Select the policy to be removed.
4. Click **Delete**.
5. Click **OK** to confirm that you wish to remove the policy.

Supplicant configurations

Supplicant configurations define an SSID and security parameters required to configure the native supplicant available on a connecting host as part of its operating system. The supplicant configuration that is used for a particular host is determined by the pairing of a supplicant configuration and a user/host profile within a supplicant policy.

When a host connects to the network and requires the use of a supplicant, the host and user data are compared to each supplicant policy starting with the first policy in the list. When a policy is found where the host and user data match the user/host profile in the policy, that policy is applied. The supplicant configuration contained within that policy configures the supplicant on the host.

The host supplicant configuration setup process is as follows:

1. Host connects to the network.
2. Host connects to an open SSID based on the operating system of the host. If authenticating through LDAP, the user must be in the selected directory group configured in the SSID mapping. You configure SSID mapping with a supplicant configuration.
3. If the user is on a Windows or macOS device, the user downloads either the Persistent Agent or the Dissolvable Agent. The agent applies the Supplicant Configuration after scanning and registering the host.
4. If the user is on an Android device, the user downloads and runs the Mobile Agent. The agent applies the Supplicant Configuration after scanning and registering the host. See [Mobile Agent on page 506](#) for download requirements.
5. FortiNAC compares user and host data to supplicant policies and finds the first match starting from the top of the list of policies.
6. The user registers or authenticates.
7. The supplicant configuration is applied.
8. The Agent attempts to move the host to the SSID that was just configured.

Settings

An empty field in a column indicates that the option has not been set.

Field	Definition
Name	User defined name for the configuration.
SSID	Name of the SSID being configured. This is not necessarily the SSID to which the host is connected. However, the agent will attempt to move the host to this SSID when the configuration is applied.  A host can have supplicant configurations stored for multiple SSIDs.
Security	Indicates the type of encryption that will be used for connections to this SSID. Options include: • Open • WEP (PSK) • WPA (PSK) • WPA2 (PSK)

Field	Definition
	• WEP Enterprise (PEAP) • WPA Enterprise (PEAP) • WPA2 Enterprise (PEAP)  WPA Enterprise and WPA2 Enterprise are limited to PEAP-MSCHAPv2.
Cipher	Encryption/decryption method used in conjunction with the information in the Security field to secure this connection. Options include: • AES • NONE • TKIP
EAP Type	Currently only PEAP is supported.
Note	User specified note field. This field may contain notes regarding the conversion from a previous version of FortiNAC.
Last Modified By	User name of the last user to modify the record.
Last Modified Date	Date and time of the last modification to this configuration.
Right click options	
Delete	Deletes the selected Supplicant Configuration.
In Use	Indicates whether or not the selected configuration is currently being used by any other FortiNAC element. See Configurations in use on page 603 .
Modify	Opens the Modify Supplicant Configuration window for the selected configuration.
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746.  You must have permission to view the admin auditing log. See Add an administrator profile on page 139 .

Create or edit a configuration

1. Select **Policy & Objects**.
2. Expand **Supplicant EasyConnect**.
3. Select **Configuration**.
4. On the **Supplicant Configurations** window, click **Create New** or select an existing configuration and click **Edit**.
5. Enter a name for this configuration.
6. Enter an SSID.

7. In the **Security** field, select a type from the drop-down list. Options include: Open, WEP, WPA, WPA2, WEP Enterprise, WPA Enterprise, WPA2 Enterprise.
8. Click in the **Password** field to open the Password pop-up. This is the Pre-Shared Key. Enter the key twice to confirm that it is correct and click **OK**. The Password field does not display if Open, WPA2 Enterprise or WPA Enterprise is selected in the Security field.
9. Click in the **Cipher** field and select AES, NONE or TKIP.
10. In the **EAP Type** field, PEAP is the only option. EAP type does not display when Open, WEP or WPA is selected in the Security field.
11. The **Validate Server Certificate** field applies only to Windows 7 and higher hosts.
 - If disabled, it disables the Validate Server certificate setting on the host and any certificate will be accepted.
 - If enabled, the host validates the certificate with the list of Trusted Root certificate Authorities listed in the host's certificate Manager. If the CA is not listed on the host, the user may have to connect to the secure SSID manually.
12. If you have enabled WEP Enterprise, WPA Enterprise or WPA2 Enterprise the **CA Certificate** field is displayed. Browse to the CA or Root certificate from the CA that issued the SSL certificate used on your RADIUS server. Select the file and click Open.
13. The **CA Fingerprint** field is displayed and automatically populated after a CA or Root certificate is uploaded and the supplicant configuration is saved.
14. The **Note** field is optional.
15. Click **OK** to save the configuration.

Settings

Field	Definition
Name	User defined name for the configuration.
SSID	Name of the SSID being configured. This is not necessarily the SSID to which the host is connected. However, the agent will attempt to move the host to this SSID when the configuration is applied. A host can have supplicant configurations stored for multiple SSIDs.
Security	Indicates the type of encryption that will be used for connections to this SSID. Options include: • Open • WEP (PSK) • WPA (PSK) • WPA2 (PSK) • WEP Enterprise (PEAP) • WPA Enterprise (PEAP) • WPA2 Enterprise (PEAP) WPA Enterprise and WPA2 Enterprise are limited to PEAP-MSCHAPv2.
Password	Opens the Password pop-up. This is the Pre-Shared Key. Enter the key twice to confirm that it is correct and click OK. The Password field does not display if Open, WPA2 Enterprise or WPA Enterprise is selected in the Security field. The XML predefined characters ' " < > & are not supported.

Field	Definition
Cipher	Encryption/decryption method used in conjunction with the information in the Security field to secure this connection. Options include: • AES • NONE • TKIP
EAP Type	Currently only PEAP is supported.
Validate Server Certificate	Applies only to Windows 7 and higher hosts. Default = Disabled. If disabled, it disables the Validate Server certificate setting on the host and any certificate will be accepted. If enabled, the host validates the certificate with the list of Trusted Root certificate Authorities listed in the host's certificate Manager. If the CA is not listed on the host, the user may have to connect to the secure SSID manually.
CA Fingerprint	Fingerprint parsed from the CA or Root certificate from the CA that issued the SSL certificate used to secure the RADIUS server. This field does not display until after the certificate has been uploaded and the supplicant configuration has been saved.
CA Certificate	This field is only displayed if you select WEP Enterprise, WPA Enterprise or WPA2 Enterprise in the Security field. Select Choose File to browse to and select the CA or Root certificate from the CA that issued the SSL certificate used to secure the RADIUS server. CA or Root certificates can be downloaded from the CA web site. Either PEM or binary format can be used.
Notes	User specified note field. This field may contain notes regarding the conversion from a previous version of FortiNAC.

Configurations in use

To find the list of FortiNAC features that reference a specific supplicant configuration, select the Configuration from the **Supplicant Configurations View** and click **In Use**. A message is displayed indicating whether or not the Configuration is associated with any other features. If the Configuration is referenced elsewhere, a list of each feature that references the Configuration is displayed.

Delete a configuration

If a configuration is in use by another feature in FortiNAC, it cannot be deleted. A dialog displays with a list of the features in which the configuration is used. Remove the association between the configuration and other features before deleting the configuration.

1. Click **Policy & Objects**.
2. Expand **Supplicant EasyConnect**.
3. Select **Configuration**.
4. Select the configuration to be removed.
5. Click **Delete**.
6. Click **OK** to confirm that you wish to remove the configuration.

Passive Agent

Passive Agent registration allows you to create customized configurations that register and scan hosts associated with network users contained in your LDAP or Active directory. Scanning requires an agent; however, the agent does not need to be installed by the user. The agent is provided using an external method, such as Group Policy Objects, and launched when the user logs into the domain. Users experience a slight delay while logging in but are unaware that their hosts are being scanned.

When a user connects to the network and logs in, FortiNAC determines the directory group to which the user belongs. Based on that group, a Passive Agent configuration is used. The configuration registers the user and the associated host in FortiNAC. If enabled, the agent scans the host to verify that it is in compliance with the appropriate endpoint compliance policy. The scan can be specified in the configuration or determined by FortiNAC based on the user/host profile of the user or host.

Registration

To implement Passive Agent registration, you must complete the following tasks:

- Integrate your directory with FortiNAC. See [Directories on page 868](#) for configuration and integration information.
- Create one or more Passive Agent configurations. See [Add or modify configuration on page 606](#).
- If the **Passive Agent Configuration Modified** event is enabled, the Event Log tracks each Passive Agent configuration as it is added, modified or removed. In addition, the user name of the user who made the changes and the current configuration settings are included in the event message. See [Event management on page 772](#) to enable or disable this event. See [Events on page 749](#) to view the event log.
- If you plan to scan users' computers when they log in, create one or more security policies. See [Policies on page 531](#).
- If you have more than one FortiNAC and you want to control which server responds to which hosts, configure IP address ranges for each server. See [IP ranges on page 607](#).
- Go to the Agent Distribution window and download the Passive Agent. It is recommended that you rename this file, and remove the spaces in the filename before you distribute it. See [Agent packages on page 992](#).
- To scan user's computers the agent downloaded in the previous step must be set up to deploy or to be served to the host when the user logs into or off of the network. The agent can be served using Group Policy Objects, Desktop Management Software or any method that allows the network administrator to deploy and run the agent on a remote host as users login or logout of the domain. The method of deployment is up to the Network Administrator.
- If you choose to use Group Policy Objects to deploy the agent, you must also download the Administrative Templates provided on the Agent Distribution window, install them on your Windows Server and configure the appropriate settings. See [Administrative templates for GPO on page 608](#).
- When the Passive Agent is run using a script, there are additional arguments that must be used to indicate whether the agent is attempting login or logout. See [CLI arguments on page 615](#).

Manage configurations

The **Passive Agent Configurations** window displays the set of configurations you have created. Use this window to add, modify or delete configurations. Disabled configurations are ignored when users log in.

Settings

Field	Definition
Table configuration	
Rank Buttons	Moves the selected configuration up or down in the list. If a user matches more than one configuration based on the selected directory group, the configuration with the higher rank is used. One is the highest rank.
Enable Buttons	Enables or disables the selected configuration. Disabled configurations are ignored when a user logs onto the network.
Table columns	
Enabled	A green check mark indicates that the configuration is enabled. A red circle indicates that the configuration is disabled.
Rank	Configuration's rank in the list of configurations. Rank controls the configuration used if a user matches more than one configuration based on the selected directory group.
Name	Name for the configuration.
Register As	Indicates whether the host will be registered based on the login name of the user as a host or based on hostname as a device.
Applied Group	Directory group to which this configuration will be applied. Users within this group are registered in FortiNAC and scanned based on the rules in the associated configuration. If this is not enabled in the configuration, the word Any is displayed, indicating that directory group is not used to select the appropriate configuration. It is recommended that such a configuration be placed at the end of the list as a catch all because it could apply to a large group of users.
Scan	Indicates whether scanning is enabled or disabled. When scanning is enabled, the scan can be repeated the next time the user logs in or out if the time interval shown has been exceeded.
Scan Policy	Scan used to evaluate the host when this configuration is applied. Either a specific scan or the scan contained in the endpoint compliance policy selected by FortiNAC based on the user/host profile.
Add To Groups	FortiNAC groups where hosts are added as they log in.
Last Modified By	User name of the last user to modify the configuration.
Last Modified Date	Date and time of the last modification to this configuration.
Right click options	
Export	Exports data to a file in the default downloads location. File types include CSV, Excel, PDF, or RTF. See Export data on page 116 .
Copy	Copy the selected Configuration to create a new record.
Delete	Deletes the selected Configuration.
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746 .

Field	Definition
	 You must have permission to view the admin auditing log. See Add an administrator profile on page 139 .
Modify	Opens the Modify Configuration window for the selected configuration.
IP Ranges Button	Configures the host IP addresses that this FortiNAC server will respond to when a host logs on to or off of the network. If this is not configured, requests are accepted from all hosts.
Test Button	Allows you to test a single directory user, based on user name to determine which configuration would apply to that user on login or logout.

Add or modify configuration

1. Select **Policy & Objects > Passive Agent**.
2. Click **Add** or select a configuration and click **Modify**.
3. Refer to the table below for information on each option for this window.
4. Click **OK** to save.

Agent selections contained within the endpoint compliance policy used to scan the host are ignored when the Passive Agent is used. The Passive Agent scan will only occur if there is a connected adapter, or if the scan name is provided in the Passive Registration Configuration.

Settings

Field	Definition
Enable	Enables or disables this configuration. Disabled configurations are ignored when a user logs onto the network.
Name	Name for the configuration.
Apply to Members of Group	Directory group to which this configuration will be applied. Users within this group are registered in FortiNAC and scanned based on the rules in the associated configuration. If this is not enabled, the word Any is displayed on the list of configurations, indicating that directory group is not used to select the appropriate configuration. It is recommended that such a configuration be ranked at the end of the list as a catch all because it could apply to a large group of users.
Register As	Indicates whether the host will be registered as a host based on the login name of the user or based on the hostname as a device with no user association.
Scan Unless Previously Scanned Within	Enables scanning. The time interval determines whether or not the host is scanned the next time the user logs on or off. For example, if the time interval is one hour and the user logs out after 30 minutes, the host is not scanned again. If the user remains logged out for two hours and then logs back in again, the host is scanned because the time interval has been exceeded. Only login and logout after the selected time interval has elapsed trigger scans.

Field	Definition
System Assigned Scan	If this option is selected the endpoint compliance policy used to select the scan is determined by FortiNAC based on the user/host profile associated with the policy.
Specific Scan	If this option is selected the scan in the drop-down list is used to scan the host regardless of the host state. Scans in the drop-down list are created in Policy Configuration under Endpoint Compliance . See Add or modify a scan on page 547 .
Add To Groups	FortiNAC groups to which hosts are added as they log in. If new groups are added to the list, the host is added the next time the user logs in. If groups are removed from this field, the host is not removed from those groups automatically. You must remove the host manually from the Groups View. See Groups on page 843. Click Select to view or modify the list of groups. On the Select Groups window, the All Groups column displays a list of available groups and the Selected Groups column displays a list of the groups to which hosts will be added. Use the arrows in the center of the window to move groups from one column to the other.

Delete configuration

1. Select **Policy & Objects > Passive Agent**.
2. Select a configuration and click **Delete**.
3. A message displays asking if you are sure. Click **Yes** to continue.

Copy configuration

1. Select **Policy & Objects > Passive Agent**.
2. Select a configuration and click **Copy**.
3. The **Add Configuration** window displays with the information from the selected configuration.
4. You must, at minimum, modify the name of the configuration. Modify other fields as needed and click **OK** to save.
5. For settings, see [Add or modify configuration on page 606](#).

IP ranges

Under the **Passive Agent Configurations** window, you have the option of limiting the FortiNAC to hosts from within selected IP address ranges. If you have multiple FortiNAC servers, you can control which servers respond to which user login/logout requests based on the IP address of the host connecting to the network. If IP address ranges are configured on this server it will only respond to requests from hosts within the range. If no IP address ranges are configured, the server responds to all requests.

Configure IP ranges

1. Select **Policy & Objects > Passive Agent**.
2. Click **IP Ranges**.
3. Click **Add** to add an IP address Range. Enter the Starting and Ending IP addresses and click **OK**.

4. To modify a range, select it from the list and click **Modify**.
5. To delete a range, select it from the list and click **Delete**.
6. When the ranges are configured correctly, click **Close**.

Test IP addresses

Use **Test** to test an individual IP to make sure it is contained within one of the IP address ranges in the list.

1. Select **Policy & Objects > Passive Agent**.
2. Click **IP Ranges**.
3. Click **Test**.
4. Enter a single IP address and click **OK**.
5. A message is displayed indicating either **IP Passed** or **IP Failed**. If the IP failed, you must either update your ranges or configure the appropriate range on a different FortiNAC.

Test a directory user

You can test a single directory user and determine which configuration would apply to that user on login or logout. The test tool takes a sample user and tries to match that user with a configuration. Users are matched to configurations based on the directory group in the Applied Group field. Users may match more than one configuration depending on the groups in which they are members. If a user matches more than one configuration, the configuration with the highest rank is used. The lower the rank number the higher the rank, for example a configuration with Rank 1 would be the highest on the list. Disabled configurations are ignored. Run the test as follows:

1. Select **Policy & Objects > Passive Agent**.
2. Click **Test** at the bottom of the window.
3. Enter the **User Name** and **Domain Name** of your sample user.
4. Click **OK** to display the results of the test. If the user matched a configuration because they were a member of the associated directory group, the name of the configuration displays in the Test Configuration window. If the user did not match any configuration, the Testing Configuration window displays No Configuration Found.

Administrative templates for GPO

Administrative templates are used to configure registry settings on Windows endpoints through Group policy objects. For the Persistent Agent and the Passive Agent, there are templates to configure the Server URL of the FortiNAC Application Server with which the agent will communicate. There are also per-computer and per-user templates to enable or disable the system tray icon or Balloon Notifications of status changes. The Balloon Notification template does not affect the Server IP and is not required.

FortiNAC does not support an Administrative Template for deploying configuration changes to macOS computers or users through GPO. You can investigate 3rd party applications, such as Likewise Enterprise that support macOS computers using Group Policy Object editor. The modifications shown in the tables below can be made in the Preferences file on macOS hosts, using the tool of your choice.



The Persistent Agent running on a macOS computer can determine the server to which it should connect via DNS server records it does not require changes to Preferences.

If you are using the Persistent Agent, your Windows login credentials are automatically passed to FortiNAC. You can modify the Administrative Template to hide the Persistent Agent Login dialog and use the Windows login credentials sent by the Persistent Agent by modifying the settings in the Administrative Template. See [Using Windows domain logon credentials on page 502](#).

Security is enabled by default. It is recommended that you update to the latest template files and configure the templates for the new security settings.

Requirements:

- Active Directory
- Group Policy Objects
- Template Files From Fortinet

Templates:

The templates listed below are provided by Fortinet. You must run the installation program for the templates on your Windows server. Be sure to select the appropriate MSI for your Windows server architecture.

- 32-bit (x86): Bradford Networks Administrative Templates.msi
- 64-bit (x86_64): Bradford Networks Administrative Templates-x64.msi

Install a GPO template

1. In FortiNAC, select **System > Settings > Updates > Agent Packages**.
2. At the top of the Agent Distribution window click either the **32-bit (x86)** or the **64-bit (x86_64)** link to download the appropriate template file.
3. Copy the template file to the domain server.
4. On the domain server, double-click the msi file to start the installation wizard.
5. Click through the installation wizard. When installation has completed, the Microsoft Group Policy Management Console is required to complete the installation. Refer to the Windows Server documentation for details.
6. Navigate to the **Group Policy Object** you want to edit, right-click and select **Edit** to display the GPO Editor pane.
7. Right-click **Computer Configuration > Administrative Templates** and select **Add/ Remove Templates**, shows the current templates pop-up.
8. Click **Add** and browse to `Program Files\Bradford Networks\Administrative Templates`.
 - a. To use the Persistent Agent, select `FortiNAC Persistent Agent.adm` and click **Open**.
 - b. To use the Passive Agent, select `FortiNAC Passive Agent.adm` and click **Open**.
9. Click **Close**, and the Administrative Templates will be imported into the GPO.

Install an updated template with balloon notifications

If you already have a Fortinet Administrative Template installed for the Persistent Agent and the Balloon Notifications were ever set to anything other than Not Configured (e.g. enabled or disabled), you must unconfigure the Balloon Notifications and push the settings to your clients. When your clients have all been updated, then the new template can be installed. These templates affect the registry settings on the client host. In the case of the Balloon Notifications, removing the previous configuration before installing the new one ensures that the keys will be set correctly.

Before updating a template, be sure to record the current template settings. Existing template settings are lost when the new template is installed.

1. In FortiNAC, navigate to **System > Settings > Persistent Agent**.
2. Select **Properties** and make sure that Display Notifications is disabled. When you have uploaded and configured the new template, come back to this view and restore the Display Notifications option to its original state.
3. Log into your Windows server and open the **Group Policy Management Tool**.
4. Navigate to the **Group Policy Object** you want to edit, right-click and select **Edit** to display the GPO Editor pane.
5. Select **Computer Configuration > Administrative Templates > Bradford Persistent Agent**.
6. In the pane on the right, right-click on the Balloon Notifications setting and select Properties.
7. On the **Setting** tab in the **Properties** window, select **Not Configured** and click **OK**.
8. When all of your clients have received the updated settings, the new template can be installed.
9. Navigate to the **Group Policy Object** you want to edit, right-click and select **Edit** to display the **GPO Editor** pane.
10. Right-click **Computer Configuration > Administrative Templates** and select **Add/ Remove Templates** to show the current templates pop-up.
11. Select the old template and click **Remove**. Follow the instructions in [Install a GPO template on page 609](#) to install the new template.

Install an updated template without balloon notifications



Before updating a template, be sure to record the current template settings. Existing template settings are lost when the new template is installed.

1. On your Windows server, open the Group Policy Management Tool.
2. Navigate to the **Group Policy Object** you want to edit, right-click and select **Edit** to display the **GPO Editor** pane.
3. Right-click **Computer Configuration > Administrative Templates** and select **Add/ Remove Templates** to show the current templates pop-up.
4. Select the old template and click **Remove**. Follow the instructions in [Install a GPO template on page 609](#) to install the new template.

Modify template settings

See the table below for settings which can be configured using the Administrative Templates provided.

Settings

Option	Definition
Persistent Agent template	
Balloon Notifications	Enables or Disables Balloon Notifications on a per-host or per-user basis. This setting is not required for configuring Server IP information. Options include: • Enabled: Forces balloon notifications for host state changes to be enabled on the

Option	Definition
	host. • Disabled: Forces balloon notifications for host state changes to be disabled on the host. • Not Configured: Use the non-policy setting (Enabled).
Login Dialog	Enables or Disables the login dialog on a per-host or per-user basis. This setting is not required for configuring Server IP information. See Using Windows domain logon credentials on page 502 for further instructions. Options include: • Enabled: The login dialog is enabled. This can be used per-user to override a per-host setting of Disabled. • Disabled: The login dialog is disabled. The agent will never prompt the user for credentials. This is useful in certain Single-sign-on configurations. • Not Configured: The login dialog is enabled, unless overridden by a per-user configuration.
System Tray Icon	Enables or Disables the system tray icon on a per-host or per-user basis. This setting is not required for configuring Server IP information. (Requires Persistent Agent 2.2.3 or higher). Options include: • Enabled: The system tray icon is enabled. This can be used per-user to override a per-host setting of Disabled. • Disabled: The system tray icon is disabled. Disabling the system tray icon also disables the following functionality: Status Notifications (Show Network Access Status, Login, Logout), Message Logs and the About dialog. • Not Configured: The system tray icon is enabled, unless overridden by a per-user configuration.
Max Connection Interval	The maximum number of seconds between attempts to connect to FortiNAC.
Security settings	
Security Mode	Indicates whether security is enabled or disabled.
Home Server	Server with which the agent always attempts to communicate first. Protocol configuration change requests are honored only when they are received from this server. If this servers is not set, it is automatically discovered using Server Discovery. On upgrade, this is populated by the contents of ServerIP.
Limit Connections To Servers	Enabled: Agent communicates only with its Home Server and servers listed under Allowed Servers list displayed. Disabled: Agent searches for additional servers when the home server is unavailable. Allowed Servers List: In large environments there may be more than one set of FortiNAC servers. If roaming between servers is limited, list the FQDNs of the FortiNAC Application Servers or FortiNAC Servers with which the agent can communicate.
Passive Agent template	
Passive Agent	Server URL List: Comma separated list of URLs (HTTP(s)://<server_name>/<context> formatted) for the FortiNAC servers that hosts running an agent should contact. Hosts must be able to reach all of the URLs in order to run properly.

Option	Definition
	Example: http://qa228/registration The context portion of the Server URL is the area of the captive portal the agents should contact, such as registration, remediation, or authentication.

Registry keys

The template setup shown in the table above modifies the Windows host's registry settings. The table below shows the modifications made to the host's registry keys by the Group Policy Object using the administrative template. If you use a tool other than GPO, you must make sure to set the appropriate keys on each host.

Upon installation of the Persistent Agent, the following key is created by default (and can be viewed using the Windows registry editor on the endstation):

```
HKLM\Software\Bradford Networks\Client Security Agent
```

When registry settings are pushed to a host via software, one or both of the following keys are created (depending upon the values pushed):

```
HKEY_USERS\ ... \Software\Policies\Bradford Networks\Persistent Agent
HKLM\Software\Policies\Bradford Networks\Persistent Agent
```

When the settings are pushed, the values for HKLM\Software\Bradford Networks\Client Security Agent will remain the same, but any settings altered via the software push will override those listed in the original key.

On 64-bit operating systems in RegEdit, these registry values will appear in the following key:

```
HKLM\Software\wow6432node.
```

Key	Value	Data
Persistent Agent		
HKLM\Software\Policies\Bradford Networks\Persistent Agent	ServerIP	The fully qualified hostname to which the agent should communicate. Data Type: String Default: Not Configured
HKLM\Software\Policies\Bradford Networks\Persistent Agent	ClientStateEnabled	0: Do not show balloon notifications on status changes. 1: Show balloon notifications on status changes. Data Type: DWORD Default: Not Configured
HKEY_USERS\ ... \Software\Policies\Bradford Networks\Persistent Agent	ClientStateEnabled	0: Do not show balloon notifications on status changes. 1: Show balloon notifications on status changes. Data Type: DWORD Default: Not Configured

Key	Value	Data
HKLM\Software\Policies\Bradford Networks\Persistent Agent	LoginDialogDisabled	0: Enable Login Dialog. 1: Disable Login Dialog. Data Type: DWORD Default: Not Configured (Login Dialog displayed)
HKEY_USERS\ ... \Software\Policies\Bradford Networks\Persistent Agent	LoginDialogDisabled	0: Enable Login Dialog. 1: Disable Login Dialog. Data Type: DWORD Default: Not Configured (Login Dialog displayed)
HKEY_USERS\ ... \Software\Policies\Bradford Networks\Persistent Agent	ShowIcon	0: Do not show the tray icon. 1: Show the tray icon. Data Type: DWORD Default: Not Configured (Tray icon displayed)
HKLM\Software\Policies\Bradford Networks\Persistent Agent	ShowIcon	0: Do not show the tray icon. 1: Show the tray icon. Data Type: DWORD Default: Not Configured (Tray icon displayed)
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Bradford Networks\Persistent Agent	maxConnectInterval	The maximum number of seconds between attempts to connect to FortiNAC. Data Type: Integer Default: 960
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Bradford Networks\Persistent Agent	securityEnabled	0: Disable Agent Security. 1: Enable Agent Security Data Type: Integer Default: 1
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Bradford Networks\Persistent Agent	homeServer	The fully qualified hostname of the default server with which the agent should communicate. Data Type: String Default: Empty
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Bradford Networks\Persistent Agent	restrictRoaming	0: Do not restrict roaming. Allow agent to communicate with any server. 1: Restrict roaming to the home server and the allowed servers list. Data Type: Integer

Key	Value	Data
		Default: 0
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Bradford Networks\Persistent Agent	allowedServers	Comma-separated list of fully qualified hostnames with which the agent can communicate. If restrict roaming is enabled, the agent is limited to this list. The home server does not need to be included in this list (for example, a.example.com, b.example.com, c.example.com). Data Type: String Default: Empty
Passive Agent		
HKEY_USERS\{SID}\Software\Policies\Bradford Networks\PASSIVE	ServerURL	Server URL List: Comma separated list of URLs for the FortiNAC servers that an agent should contact. Example: http://qa228/registration The context portion of the Server URL is the area of the captive portal the agents should contact, such as registration, remediation, or authentication.
HKLM\Software\Policies\Bradford Networks\PASSIVE	ServerURL	Server URL List: Comma separated list of URLs for the FortiNAC servers that an agent should contact. Example: http://qa228/registration The context portion of the Server URL is the area of the captive portal the agents should contact, such as registration, remediation, or authentication.

Deploy the Passive Agent

1. On your Windows server open the Group Policy Management Tool.
2. Navigate to the Group Policy Object you want to edit.
3. Right-click the Group Policy Object and select **Edit** to display the GPO Editor pane.
4. Click **User Configuration > Policies > Windows > Settings Scripts (Logon/Logoff)** to display the Logon and Logoff script configurations.
5. Double click **Logon** for Logon Properties.
6. Click **Add** and then browse to the location of `FortiNAC_Passive_Agent.exe`.
7. Select `FortiNAC_Passive_Agent.exe` to add it to the **Script Name** field.

8. Enter `-logon` in the **Script Parameters** field.

9. Click **OK**.

To ensure the user is logged off the host upon logging out, do the following:

1. Follow steps 1-4, and then double-click **Logoff**.

2. Add `FortiNAC_Passive_Agent.exe` to the Script Name field, and then enter `-logoff` in the Script Parameter field.

3. Click **OK**.

CLI arguments

The Passive Agent is designed to be run via an external script when a user logs onto or off of the network. Creating the script is the responsibility of the Administrator. When running the agent CLI arguments that indicate whether the agent is attempting to logon or logoff. If no argument is used, the agent defaults to login. Arguments are case sensitive.

Type	Arguments	Description
Logon	<code>-login</code> <code>/login</code> <code>-logon</code> <code>/logon</code> <code>-on</code> <code>/on</code> <code>-in</code> <code>/in</code> <code>-authenticate</code> <code>/authenticate</code>	Any one of these arguments can be used to indicate Logon. There must be a space between the name of the agent file and the argument. Example: <pre>FortiNAC_Passive_Agent.exe -login</pre>
Logoff	<code>-logout</code> <code>/logout</code> <code>-logoff</code> <code>/logoff</code> <code>-off</code> <code>/off</code> <code>-out</code> <code>/out</code> <code>-deauthenticate</code> <code>/deauthenticate</code>	Any one of these arguments can be used to indicate Logoff. There must be a space between the name of the agent file and the argument. Example: <pre>FortiNAC_Passive_Agent.exe -logout</pre>

Remediation configurations

Use the Remediation Configuration to set up the Admin Scan Configurations used for options such as denying access to guests or other users by time of day or day of week.

To manage scans, you can add, modify, and remove scan scripts and profiles. You may also view performance statistics for the scan scripts and profiles. Schedule scans from the Modify Scan dialog box.

Add a scan

1. Click **Policy & Objects > Remediation Configuration**.
2. Click **Add**.
3. Use the settings in the table below to enter the parameters for the script or profile you are adding.
4. Click **Apply**.

Settings

Field	Definition
Type	The type of scan you are adding: • System - These scans runs scripts on the FortiNAC platform. • Admin - These scans indicate the reason why a host was manually marked at risk. They are not actually scanning the host but provide a configuration or profile with which to associate the host state. Admin Scans are also used to mark hosts At Risk or Safe based on an alarm action triggered by an event.
Script/Profile	System scripts • ForceCSARescan - Forces the Target Group of hosts using the Adapters cannot be successfully moved between hosts using the Dissolvable Agent. to be rescanned by setting the hosts in the group to At-Risk. • ForcePersistentAgent - Forces the Target Group of hosts using the Persistent Agent to be rescanned by setting the hosts in the group to At-Risk. • PassAllClients - Sets the Target Group of hosts to Safe. • FailAllClients - Sets the Target Group of hosts to AtRisk. Admin scans Enter a name for the scan. This scan is initiated on the Host Properties under the Health tab.
Label	Displayed on the failure page when a network user's PC has failed a scan. If no label is provided, the scan name is used. The label or scan name is a link that takes the user to a page indicating why the PC has failed the scan.
Max Scan Execution Time (sec)	The maximum length of time FortiNAC will wait for the scan to return a status of passed or failed. If the elapsed time is greater than this value, a script failed error is generated and the host returns to the queue of hosts waiting to be scanned.
Status	Enable or Disable the scan. This setting can be modified to allow the scan to run or to stop it from running.
Target	The sub-set of FortiNAC hosts that will be scanned. • All Hosts • All Hosts & Servers • All Registered • All Rogues • All Servers • All VPN Clients

Field	Definition
	- Group: See below. - Security and Access Attribute Value. See below.
Group	Specify the FortiNAC host group to be scanned. This option is only available if you select Group as the Target.
Security and Access Attribute Value	Used to determine which scan is to be applied to hosts connecting to the network whose associated user has this value set in the Active Directory Security and Access attribute. The host inherits this value from the user. This option is only available if you select Directory Attribute as the Target .
Patch URL	The location of the URL containing instructions for users whose hosts fail the scan. This must be a local URL.
Patch Information	If a host has failed a scan, the user must remedy the issue and rescan. Use this second field to provide the user with a brief set of instructions. For this field to be displayed to the user, you must use the portal pages distributed with FortiNAC and the Use Portal Version 1 check box on the portal configuration window must be disabled.

View scan status

1. Click **Policy & Objects > Remediation Configuration**.
2. Click the radio button next to a script/profile.
3. Click **View**. The **Scan Status** window is displayed.

Settings

Field	Definition
Script/Profile	Name of the scan.
Type	The type of scan.
Target	Sub-set of FortiNAC hosts that are being scanned by this script or profile.
Execution Time (sec)	Maximum length of time FortiNAC waits for the scan to return a status of passed or failed. If the elapsed time is greater than this value, a script failed error is generated and the host returns to the queue of hosts waiting to be scanned.
Servers Failed	Total number of servers that failed the scan.
Hosts Failed	Total number of hosts that failed the scan.
Elements Scanned	Number of elements scanned.
Queue Count	Number of elements waiting to be scanned.
Status	Whether the scan is Enabled or Disabled.

Click the **Details** button for additional information.

The Scan Details window displays the overall details of the scan and the specific host results for the scan.

Details settings

Field	Definitions
Script/Profile	Name of the scan.
Elements Scanned	Number of elements scanned.
Execution Time (sec)	Maximum length of time FortiNAC will wait for the scan to return a status of passed or failed. If the elapsed time is greater than this value, a script failed error is generated and the host returns to the queue of hosts waiting to be scanned.
Average Execution Time	Average length of time the scan was run against an individual host in the group being scanned.
Filter Status	Filter setting for script performance results: • All - All scanned hosts results • Safe - Only scanned hosts that are safe • At Risk - Only scanned hosts that are at risk • Script Failed - Only hosts that failed the scan
Start Record	Number of the first record to be displayed in the range of records selected.
End Record	Number of the last record to be displayed in the range of records selected.
Clear List of Scanned Hosts	Clears the list of hosts that have been scanned against this scan profile. Click Now to clear the list immediately. Click Schedule to schedule when to clear the list.
Hosts Details	Specific information on each scanned host. • Name - MAC address or name of host • IP address - IP address of host • Server - Server that performed the scan • Execution Time (sec) - The length of time in seconds that it took to run the scan against the host • Status - Safe, At Risk, or Script Failed

Click the icon next to a host name to view the Host Properties. The Health Tab provides details regarding the Scan Report for the host so you can rescan the host immediately if you want. See [Properties on page 221](#) for more information.

Clear scanned hosts list

Under Remediation Configuration - Modify or View you have the option to clear the list of Scanned Hosts. This forces the hosts in the results list to be rescanned. You may clear the list immediately or schedule the list to be cleared at specific intervals. On the Modify Scan view:

- Click **Now** to clear the list immediately.
- Click **Schedule** to set the interval that the list will be cleared.

1. Click **Policy & Objects > Remediation Configuration**.
2. Click the radio button next to a scan to select it.

-
3. Click **Modify**.
 4. Click **Schedule**.
 5. Enter the **Schedule Interval** (the **number** of minutes, hours, or days) that the scanned host list is to be cleared.
 6. Select the **time increment** from the drop-down list.
 7. Enter the **Next Scheduled Time** for the scan to run. The format for the entry is MM/DD/YY hh:mm AM/PM.
 8. Check the **Pause** option if you want to pause the scan until you run it manually from **Scheduler**. See [Scheduler on page 857](#) for more information. If you leave this option unchecked, the scan runs according to the parameters you entered.
 9. Click **Apply**.

Modify or remove a scan

1. Click **Policy & Objects > Remediation Configuration**.
2. Click the radio button next to the scan you want to select it.
3. To remove the scan, click **Remove**.
4. To modify the scan, click **Modify**. See [Add a scan on page 616](#) for settings.
5. The list of Scanned Hosts may be cleared immediately or be scheduled to be cleared at a specified interval. See [Remediation configurations on page 615](#) for additional information.
6. Click **Apply**.

Roles

Roles are used in two different ways in FortiNAC. Roles assigned to hosts managed in the Host View or Users are attributes of those elements. In this case the role is another way to group users and hosts. Roles can be used in user/host profiles to filter for specific Users or Hosts when applying network access policies, endpoint compliance policies, and Supplicant EasyConnect policies.

For devices or hosts managed in the Inventory roles are used to determine the network access given to those elements based on their connection location. In this case Roles are used with network device roles. The Role is simply a name or identifier that is assigned to the host or device. The Network Device Role maps the connection location with device, port or SSID groups to a specific Role. For example, when a device connects to the network with Role A on Switch 1, FortiNAC searches through the network device roles for a record with Role A that has a connection location containing Switch 1. The first matching Network Device Role is used. The configuration of this Network Device Role can place the device in a specific VLAN or can apply a CLI configuration.

Role management relies on the configuration of both Roles and network device roles. The **Roles** view contains the list of possible Role names and controls assigning roles to users and hosts based on group membership. Roles for hosts managed in the Host View and Users do not need a corresponding Network Device Role. Network access for those hosts and users is handled by network access policies. Roles for devices or hosts managed in Inventory require a corresponding Network Device Role to control network access. See [Roles view on page 625](#).



If a role has more than one mapping for the same device or port group, the order of precedence is determined by the order of the role mappings on the network device roles View. Starting from the top of the list, the first mapping match found is used.

See [Configuration on page 621](#) for an overview of setup requirements.

Configuration

1. Determine which device(s) will be used to support a specific role.
2. Configure the device(s) with the VLAN or Interface ID information for the role.
3. Create a device group and add the device(s) for each set of devices that will be used for roles. For example, you might have a group of devices that provide network access in Building A. That group of devices will provide different types of access than the devices in Building B, therefore you would create two separate device groups. See [Groups on page 843](#) for information on groups.
4. If only some ports on a device or devices will be used for role management, you can place just the required ports in a Port group specifically for roles. First, determine which ports will participate in role management and place those ports in the Role Based Access Group. Ports that are not in this group cannot apply roles. Once ports are in the Role Based Access group, place them in groups that will be associated with roles. See [Groups on page 843](#) for information on groups.



Ports that are assigned roles are typically included in the Role Based Access Group. If a port is assigned a role but is not included in the Role Based Access Group, devices connecting to that port are placed in the default VLAN entered on model configuration for that device. They are not placed on the VLAN defined for the role. However, if the role is used as a filter for any policy, that policy is still used.

-
5. Create a list of Roles. See [Roles view on page 625](#).
 6. Determine which hosts or users will be identified by the role.
 7. Associate the hosts or users with the role. See [Assigning roles on page 621](#).



Use only one method to associate a host or a user with a role. If more than one method is used, the role is assigned based on the ranking of roles and the first piece of data that matches.



Roles are only applied to hosts that are registered.

-
8. Once roles have been created, configure network device roles. Network device roles indicate the actions to be taken when a device in that role connects to a group of devices or ports. There can be multiple mappings for a single role. For example, Role A can have a mapping for Port/Device Group A and a different mapping for Port/Device Group B. Select the Device or Port group and enter the network access IDs. See [Network device roles on page 627](#).

Assigning roles

Roles can be assigned to users, hosts, network devices and ports. Each one of these entities has a role field on its corresponding Properties window. Assignment of roles is accomplished by setting the role field for the user, host, device or port either manually or using one of the options listed in the table.

In the event that multiple methods are used to set a role, the order of precedence is determined by the order of the roles in the Roles view. Starting from the top of the list, the first matching role is used. For example, assume you have assigned roles to hosts based on groups. Later you add the host to a new group. If that new group is associated with a role that is ranked above the host's original role, the host's role will be changed.

Roles created on the FortiNAC server will be ranked above global roles created on the FortiNAC Manager. The rank of a local role can be adjusted above or below another local role, but cannot be ranked below a global role. The rank for a global role cannot be modified from the FortiNAC server.

Settings

Setting	Definition
User roles	
User Roles Based On Groups	Users can be assigned roles by placing them in a group and then associating that group with a role in the Roles View. See Add a role for additional information on adding roles. User groups can also be created based on groups in the directory. These groups are treated the same as groups created manually within FortiNAC. If a user is a member of more than one group, the group that is found first when matching users to roles determines the role assigned to the user.  When assigning Roles to users, the use of directory attribute data over directory groups is recommended. Attribute data is retrieved directly from the directory as the user registers, while group information is retrieved from data cached on the FortiNAC server and could be out-dated.
User Roles Based On A Directory Field	Network users can be assigned a role based on a field in LDAP or Active Directory (attribute data). For example, you might choose to have roles based on a field in the directory called Department. The data within the Department field would be the name of the role, such as Accounting or Customer Service. In a university environment, a user might have a role based on whether he is a Student or Faculty. To assign roles based on a field in a directory you must indicate which field in the directory is to be used as a role. See to map the role field. Users in the directory with matching data in this field constitutes a group, even though the group is not shown anywhere. For example, users with Accounting in their department field are treated as an Accounting group for the purpose of assigning roles. Next, you must create a Role with the exact same name as the data contained in the directory field. For example, if the user's role in the directory is Accounting, you must create a Role in the Roles View that is named Accounting. When a user registers, the role field in User Properties is set to match the data in that user's role field in the directory.

Setting	Definition
User Roles Based On Fields In Captive Portal	When registering a host through the Captive Portal, if the user fields on the portal page have a role set, that role is assigned to the user, such as during registration or authentication.
Individual User Roles	In some situations you may want to assign a role to a single user. First create the role in the Roles View. Then, navigate to the User Properties window and modify the Role field.
Host roles	
Host Roles Inherited From Users	When registering a rogue to a user in the Hosts View, you have the option to use the user's role or to select a different role for the device. See Add or modify a host. When registering a host through the Captive Portal, if the portal does not have a role set, the host inherits the role of the user. If the user's role changes, regardless of how it is changed, any host registered to that user that has the same role will be changed also. For examples, see Use Cases chart below.
Host Roles Assigned Through Captive Portal	When registering a host through the Captive Portal, if the portal page has a role set, that role is assigned to the host during registration. If the role field is blank, the host inherits the role of the user.
Host Roles Based On Groups	Hosts can be assigned roles by associating a group with a role in the Roles view and then adding the host to that group. For examples, see Use Cases chart below. See Add a role for additional information on adding roles.
Host Roles Assigned Manually	This would typically be used to assign a role to hosts, such as a medical device that connects to the network. To register rogues and set their role: Select one or more rogues in the Hosts View. Right-click on the selected records and choose Register as Device from the menu. On the registration pop-up you can select device type and role. See Register a host as a device. To set roles for registered devices: Select one or more devices in the Hosts View. Right-click on the selected records and choose Set Host Role. Select the new role from the drop-down list in the pop-up window.
Host Roles Assigned By Device Profiler	This would typically be used to assign a role to hosts, such as a medical device that connects to the network. Devices that are hosts, such as medical devices, gaming devices, or printers can be assigned a role and a device type based on device profiling rules.

Setting	Definition
	If you are using the device profiler feature, you can create or use default rules that allow FortiNAC to determine the device type and assign the device to a role. When a new host device connects to the network it becomes a rogue because it is unknown. FortiNAC compares information received from the device with the device profiling rules in its database until it comes up with a match. Based on the parameters defined in the rule, the device is assigned a type and a role. See Profiled devices and Device profiling rules. The role assigned by device profiler takes precedence over any role associated with the vendor OUI.

Use Cases

Use Case	Expected Behavior
User and host have different roles	Portal Registration - Portal Configuration Role Field is populated: Host is assigned the role defined in the Role Field. - Portal Configuration Role Field is empty: Host inherits the user role. Host registered as a Device - Host inherits the user role if user logs into the host.
Host Roles Inherited From Users	John Doe is a student and has two registered hosts. - John Doe's Role: Student - John Doe's Host 1 Role: Student - John Doe's Host 2 Role: Gaming John Doe graduates and becomes faculty, so the University makes the change in AD and runs a directory sync. John's role is changed to Faculty. - John Doe's Role: Faculty - John Doe's Host 1 Role: Faculty - John Doe's Host 2 Role: Gaming Host 2 did not match John's original role of Student, so it is not changed.
Host is added to a group with an associated role	Host role is changed to the group role. If host is removed from the group, the host role does not change. If changing role is desired, it must be done manually.
Host is added to multiple groups, each with an associated role	Assigned role is based on ranking specified under Policy & Objects > Roles If host is removed from the group, the host role does not change. If changing role is desired, it must be done manually.
Group 1 (Role 1 associated) Group 2 (host is a member)	Add Group 2 to Group 1: Host role does not change. If changing role is desired, it must be done manually.

Remove Group 2 from Group 1: Host role does not change. If changing role is desired, it must be done manually.

Roles view

This view allows you to configure roles. Roles are assigned to Users, Hosts and Devices. For hosts managed in the Hosts View and users, roles are attributes that are used in user/host profiles as filters. For devices and hosts managed in Topology, such as a printer, roles are used to control network access based on where they connect. If you are using roles to control network access for hosts and devices, you must also configure Network Device Roles to provide a set of connection instructions for role and device or port group combinations.

For example, if Role A is assigned to all of the printers in the Accounting Department, then when a printer connects to a port in the accounting office, the Network Device Role for accounting office ports is configured to move them to VLAN 10.

In the case of a host managed in the Hosts View, if Role B is assigned to that host, then when the host connects to a port in the accounting office, FortiNAC Manager reviews the network access policies until it finds a policy for a host with Role B connected to accounting ports based on the user/host profile in the policy.

Roles can be assigned in many different ways. In the case of the Roles View, roles are assigned based on directory groups or FortiNAC Manager groups. When a user or a host is added to a group, FortiNAC Manager searches the list of roles for a match starting with the role ranked number 1. When a match is found, the role is assigned to the user or the host. In the case of directory attributes, when a user is registered and FortiNAC Manager checks the list of roles, a role with a name that exactly matches the attribute will be assigned to the user if it is the first piece of data about the user that matches the role criteria.

Roles created on the FortiNAC server will be ranked above global roles created on the FortiNAC Manager. The rank of a local role can be adjusted above or below another local role, but cannot be ranked below a global role. The rank for a global role cannot be modified from the FortiNAC server.

For additional information on all methods for role assignment, see [Assigning roles on page 621](#).

Settings

Field	Definition
Rank Buttons	Moves the selected role up or down in the list. Users and hosts are compared to roles in order by rank.
Set Rank Button	Allows you to type a different rank number for a selected role and immediately move the role to that position. In an environment with a large number of roles, this process is faster than using the up and down Rank buttons.

Field	Definition
Name	Name of the role. If you are assigning roles based on the directory attribute specified in attribute mappings in the Role field, the name of the role in the Roles view must match the data in the user's directory attribute. For example, if the directory attribute is department and the user's field is set to Accounting, then the role name must be Accounting in order to match.
Groups	One or more groups whose members will be assigned to this role. List includes Groups both in FortiNAC and in the directory, if one is being used with FortiNAC. If no groups are selected, None is displayed in this field. This effectively disables the role for group assignment. However, the role can still be assigned manually, by device profiler or through the Captive Portal.
Note	User specified note field. This field may contain notes regarding the conversion of roles from a previous version of FortiNAC.
Last Modified By	User name of the last user to modify the role. SYSTEM indicates that the role was modified by FortiNAC itself.
Last Modified Date	Date and time of the last modification to this role
Right click options	
Copy	Copy the selected Role to create a new record.
Delete	Deletes the selected Role. Roles that are currently in use cannot be deleted.
In Use	Indicates whether or not the selected role is currently being used by any other FortiNAC element. See Role in use on page 627 .
Modify	Opens the Modify Role window for the selected role.
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746 .
 You must have permission to view the admin auditing log. See Add an administrator profile on page 139.	

Add a role

Once you have created and configured the host, user and device groups, create the roles associated with these groups.

1. Select **Policy & Objects > Roles**.
2. Click **Add**.
3. In the **Name** field, enter a name for the new role. If this role corresponds to an LDAP attribute value, the spelling of the role name must be an exact match for the data contained in the user's directory record and you do not need to select a group in the Groups field.
4. Click **Select** next to **Groups**. Choose one or more user or host groups by clicking on the names in the **All Groups** column and clicking the right arrow to move them to the **Selected Groups** column. Click **OK** to continue.
5. If you are creating a role that you do not want to have automatically assigned, but wish to assign manually or through the captive portal, then do not enter any groups.

6. Click in the **Note** field to add any user defined information needed for this role.
7. Click **OK** to save the role.
8. If this role will be used to control network access for hosts managed in Inventory and devices, go to the network device roles view and configure the role mapping there. See [Network device roles on page 627](#).

Modify or delete roles

You can modify the role settings as needed. All devices, users and hosts in the database are required to have a role. You cannot remove a role from these elements. You can only change the role to something else. If no role is specified devices, users and hosts default to the NAC Default role.

If a role is in use by a Device Profiling Rule, guest template, or assigned to a Host, User, or Device, the role cannot be removed from the database. If a role is simply mapped to a device based on the device's membership in a group and not assigned specifically to the device, the role can be removed.

1. Select **Policy & Objects > Roles**.
2. Select the role from the list.
3. To remove the role from the database, click **Delete**.
4. On the confirmation window, click **Yes** to remove the role.
5. If the role is in use, a warning message is displayed and the role is not deleted. Click **In Use** for a complete list of places where this role is referenced.
6. To modify the role, click **Modify**.
7. Modify settings as needed and click **OK** to save.

Role in use

To find the list of FortiNAC features that reference a role, select the role from the **Roles** view and click **In Use**. A message is displayed indicating whether or not the role is associated with any other features. If the role is referenced elsewhere, a list of each feature that references the configuration is displayed. A role can be used in the following locations:

- Network device roles
- Hosts
- Users
- Devices
- Device profiling rules
- Vendor OUIs
- Guest templates
- Scheduled tasks with an action of **Role Assignment**
- Event to alarm mappings with an action of **Host Role Action**

Network device roles

Network Devices that request network services are provided with those services based on the role assigned to the device and the connection location. Network device roles allow you to map Device Roles and connection locations to network access configurations for connecting devices. These roles apply only to hosts managed in Inventory, such as a printer, and devices.

A role can have more than one mapping to provide different results when a device with the selected role connects to a different port or device group. For example, you could map Role A to a group of ports in the Accounting Group and place connecting printers with Role A in VLAN 10. You could also map Role A to a group of ports in the Lobby Group and place connecting printers with Role A in VLAN 20. Because roles can have more than one mapping, you must determine which mapping is appropriate for each connecting device. When a device connects, each mapping is evaluated, starting with Rank 1 and working down the list until a match is found. The first match found is used.

To view network device roles, go to Policy & Objects > Network Device Roles.

Settings

Field	Definition
Rank	Allows you to adjust the rank number for a selected device role by drag and drop the entire row using the mouse.
Role	Name of the role to which this mapping applies. If Any is displayed, this indicates that the role is not being used as a selection requirement for this mapping. When set to Any, the role field is a match for all roles.
CLI	CLI configuration that will be applied. CLI configurations are applied to the port where the device connects. See CLI configuration on page 433 .
Location	One or more groups of devices or ports where the device must be connected in order for this mapping to apply. If Any is displayed, this indicates that the field has been left blank when configuring the mapping and that location is not being used as a selection requirement for this mapping. When set to Any, the location field is a match for all locations.
Access Value	Name or number of the network access identifier where the device will be placed based on its role, such as VLAN ID, VLAN Name or Aruba Role.
Note	User specified note field. This field may contain notes regarding the conversion of roles from a previous version of FortiNAC.
Last Modified By	User name of the last user to modify the mapping. SYSTEM indicates that the mapping was modified by FortiNAC itself during an upgrade.
Last Modified Date	Date and time of the last modification to this mapping.
Right click options	
Export	Exports data to a file in the default downloads location. File types include CSV, Excel, PDF, or RTF. See Export data on page 116 .
Copy	Copy the selected mapping to create a new record.
Delete	Deletes the selected mapping.
Modify	Opens the Modify Network Device Role window for the selected mapping.
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746 .

Field	Definition
	 You must have permission to view the admin auditing log. See Add an administrator profile on page 139.

Add role mappings

Network Device Role mappings tie roles to connection locations and network access options, such as VLANs.

Settings

Field	Definition
Role	If the checkbox is enabled, you can select an existing Role from the drop-down list for this mapping. If the checkbox is not enabled, this mapping is not tied to a specific role; however, the other criteria in the mapping, such as Location, must match the connecting device or the mapping will not be used. If you configure a mapping with no Role, you may want to make sure its Rank places it toward the bottom of the list of rankings. Device connections are compared to the mappings from the lowest (1) to the highest. The first match is used.
Where (Location)	One or more groups of devices or ports where the device must be connected in order for this mapping to apply. If this field has been left blank, then location will not be used as a selection requirement for this mapping. Note: FortiSwitch in Link Mode: Port groups must be used. Device groups will not match.
Notes	User specified note field. This field may contain notes regarding the conversion of roles from a previous version of FortiNAC.
Logical Network	The logical network that will be assigned to the network devices that receive this role.

1. Select **Policy & Objects > Network Device Roles**.
2. Click **Create New**.
3. Click the **Role** check box to enable the role drop-down. If this is not enabled, this mapping can apply to any device that matches the other criteria in the mapping, such as Location. The word Any displays in the Role column on the network device roles view if this box is unchecked.
4. Select a role from the drop-down list.
5. Under **Where (Location)**, choose one or more device or port groups by clicking on the names in the **All Groups** column and clicking the right arrow to move them to the **Selected Groups** column. Click **OK** to continue.
6. Add a **Logical Network**.
7. Click in the **Note** field to add any user defined information needed for this mapping.
8. Click **OK** to save the mapping.

Modify or delete role mapping

1. Select **Policy & Objects > Network Device Roles**.
2. Select the mapping from the list.
3. To remove the mapping from the database, click **Delete**.
4. On the confirmation window, click **Yes** to remove the mapping.
5. To modify the mapping, click **Modify**. See [Add role mappings on page 629](#) for settings.
6. Modify settings as needed and click **OK** to save.

Portal

Portal configuration	631
Request Processing Rules	741
Portal SSL	745

Portal configuration



FortiNAC-OS Requirement: "https" and "http" options must be included in the "set allowaccess" command. See [Open ports](#) for details.

Portal Configuration is one in a series of initial setup windows designed to help you get your FortiNAC program up and running as quickly as possible. The Portal Configuration window is used to configure the content and layout of the portal pages that network users encounter when their devices or hosts are unregistered.

The embedded Content Editor allows you to modify selected properties of your portal pages from within the user interface. These changes affect the set of portal pages shipped with FortiNAC as well as other portals created by users in content editor, and will not modify any existing custom version 1 portal pages. If you want to continue to use legacy or custom portal pages, leave the check mark in the Use Portal Version 1 check box. If you would like to use the portal pages that can be modified with the Content Editor, first modify the pages and then, remove the check mark in the Use Portal Version 1 check box.

You may only see a sub-set of the options described in this document, based on the appliance being used. If an option is not displayed on your screen, continue with the next option described.



If you are running Firmware version 2.3.3.x or higher, you will not see references to Portal Version 1 on the Portal Configuration window.

If you choose to use your original Version 1 portal pages, refer to [Version 1 settings on page 734](#) for additional information. If you choose to use the portal pages that can be edited with the Content Editor, refer to [Content editor on page 632](#).



When working in Portal Configuration, FortiNAC displays a pop-up message warning you 45 seconds before your Admin login times out and automatically logs you out of the user interface. You can choose to extend your login time by clicking Yes on the confirmation dialog or allow the system to log you out at the end of the 45 seconds by clicking No. If you are logged out automatically before saving your changes, those changes are lost.

Portal Configuration can be accessed from Portal > Portal Configuration.

Content editor

The Content Editor tab on the Portal Configuration window allows you to edit the portal pages distributed with FortiNAC. If you have existing Version 1 portal pages and you prefer not to use the ones distributed with FortiNAC, simply leave the Use Portal Version 1 option enabled on this window.

Use a separate browser to test Portal Pages. Testing pages in the same browser logs the Admin user out of the user interface.

In a High Availability environment, portal pages are copied every 10 minutes.

The URL to use for viewing a certain page is listed within the Left Column Content of the page configuration. Example:

Configuration > Registration - Standard user login page URL is http(s)://hostname.domain.tld/registration/ValidUserLogin.jsp

The Content Editor has a Overview page that lists all Version 2 portal pages on this FortiNAC. Select one of them in the overview, then you can choose to edit, copy or delete it.

The Images tab displays the images used in Portal Pages, such as the banner. Images can also be uploaded from the Images tab.

Multiple portals can be created and managed from the Content Editor Overview. Portals can be copied and then modified. The images stored in and uploaded to the Images tab are global across all portals. See [Multiple portals on page 633](#).

HTML can be used to format text that will display in the captive portal web pages. Some characters are reserved for HTML and must be entered using special character combinations, such as the & or ampersand symbol, which must be entered as & to display correctly. If you enter one of these characters, a warning is displayed reminding you that it may cause issues when rendered on the web page shown to the user. For a complete list of reserved characters and charts for replacement options, see [Using special characters on page 647](#).

You may see the same warnings when using a character in the course of formatting with HTML, such as Bold. This would trigger a warning because < and > are reserved characters.

Settings in Overview

Option	Definition
Use Portal Version 1	Indicates that the system should use the custom portal pages you created by hand. In addition, portal pages that can be modified with the Content Editor are provided with FortiNAC. This option can be enabled and disabled as needed. When enabled the original custom portal pages are used. When disabled the portal pages associated with the Content Editor are used. It is recommended that you configure the new pages first, then disable the Use Portal Version 1 option to begin using the new pages. If you disable the Use Portal Version 1 option before configuring your new pages, network users may not be able to access your network.
Copy	Copy the elements of one set of portal pages to another set. There are options to copy all elements or just the styles to create a new portal or to overwrite an existing portal. See Copy a portal on page 733.

Option	Definition
Create New	Create a new portal configuration. You can edit the portal's name, style and properties such as Window titles or login text. See Add/Edit Portal .
Edit	Edit an existing portal. See Add/Edit Portal .
Reset to Defaults	Resets all pages and page properties to their original factory defaults for the selected portal. This includes all user specified text.
Refresh	Refreshes the window and discards any unsaved changes.
Export	Allows you to export all portals with page properties, style sheets and images to a .zip file that can be imported on another FortiNAC or can be used as a backup of your portal page configuration. Each set of portal pages is stored as a single XML file within the .zip file. The .zip file can be edited to remove unwanted portals prior to importing. See Export portal content on page 647 .
Import	Allows you to select a previous export file for import. See Import portal content .
Images Tab	Displays the images for the selected portal. Uploads new images to the appropriate location for use in the selected portal. See Images on page 734 .

Multiple portals

The Portal Content Editor has options to create separate portals for different sets of users. For example, if you are a conference center and you need to run conferences for three different businesses, each business will require guest access to your network to connect to the internet. Instead of having one generic portal experience, you can create multiple sets of portal pages, each tailored to one of the businesses using your facility. Using Portal Policies you can determine which portal should be presented to a user based on host attributes, such as connection location.

By default, there are three portals you can find in the content editor overview:

- Portal, a generic portal setup
- RegistrationPortal, with several registration methods enabled by-default
- RestrictedPortal, for hosts not allowed to access the network

Any action that you perform on the Portal Content Editor only affects the portal selected in the portal editor.

Images are common to all portals.

Portal v1 pages cannot be used in a multiple portal environment. Disable Portal v1 under **Portal > Portal Configuration** and use portal v2 pages distributed with FortiNAC.

Implementation

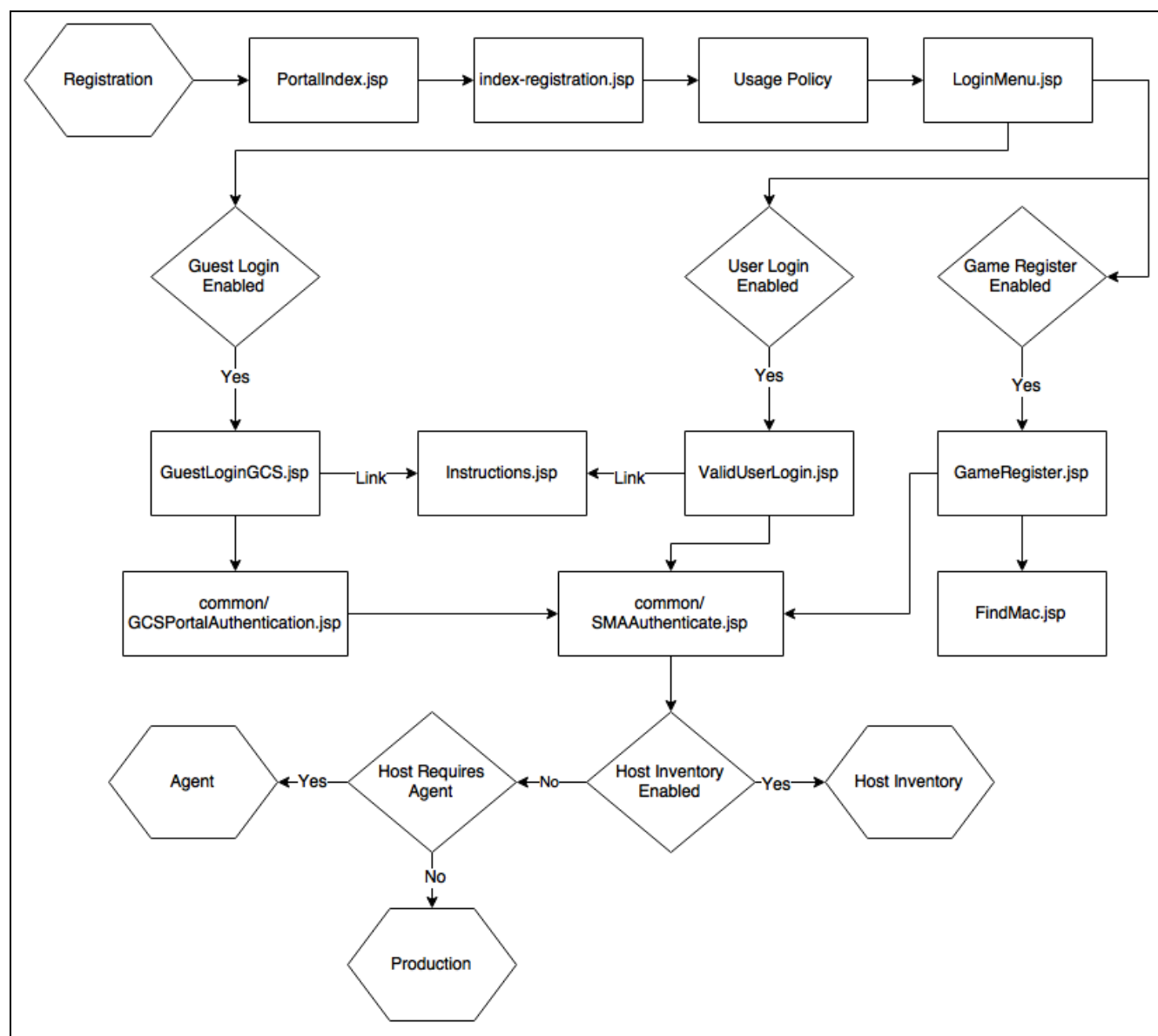
- Using the Portal Content Editor, create a basic portal and configure the elements that are common to all of your portals. This one will serve as your template. See [Content editor on page 632](#).
- In the Portal Content Editor under **Configuration > Portal Pages**, there is an Isolation section with an option to Display the Portal Selector Page. Enable this option if you want to allow a user to select a Portal when the host is in Isolation and FortiNAC cannot determine the portal for that host. Once enabled, the Portal Selector configuration page is available under **Configuration > Isolation**.

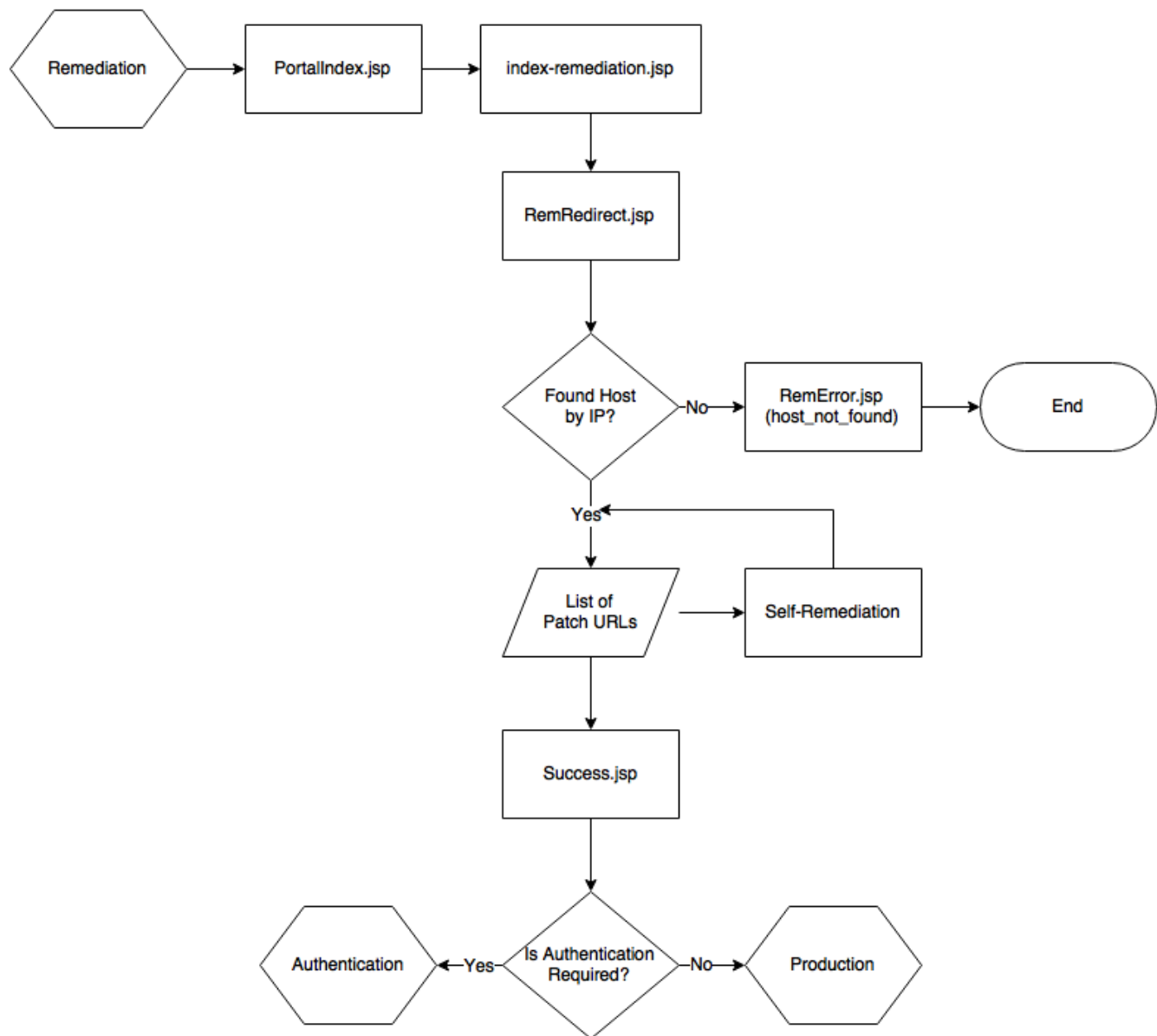
- Use the **Copy** option in the Portal Content Editor to create a new set of portal pages based on the template set and edit those elements that make the new portal unique to a particular group of users. See [Copy a portal on page 733](#).
- Select a default portal. If FortiNAC cannot determine the portal for a connecting host, the default portal is used. See [Select a default portal on page 733](#).
- Create a User/Host Profile for each separate Portal. The User/Host Profile is used to match a host with a Portal Policy based on host attributes. Note that FortiNAC can only discover a small set of information about the host when it connects to the network. Therefore, the attributes that can be used in the User/Host profile are limited for determining the portal to be used. It is recommended that you use host connection location, IP address, MAC Address and/or Operating System. See [User/host profiles on page 466](#).
- Create a Portal Policy for each separate Portal. The Portal Policy combined with the User/Host Profile determine which portal should be presented to a connecting host. See [Portal policy on page 471](#).
- Specific portals can be associated with one or more SSIDs using the options under SSID Mappings. When a portal is assigned to an SSID a corresponding User/Host Profile and Portal Policy are created. The SSID to which the host connects will determine the portal presented to the user. See [SSID mappings on page 76](#).

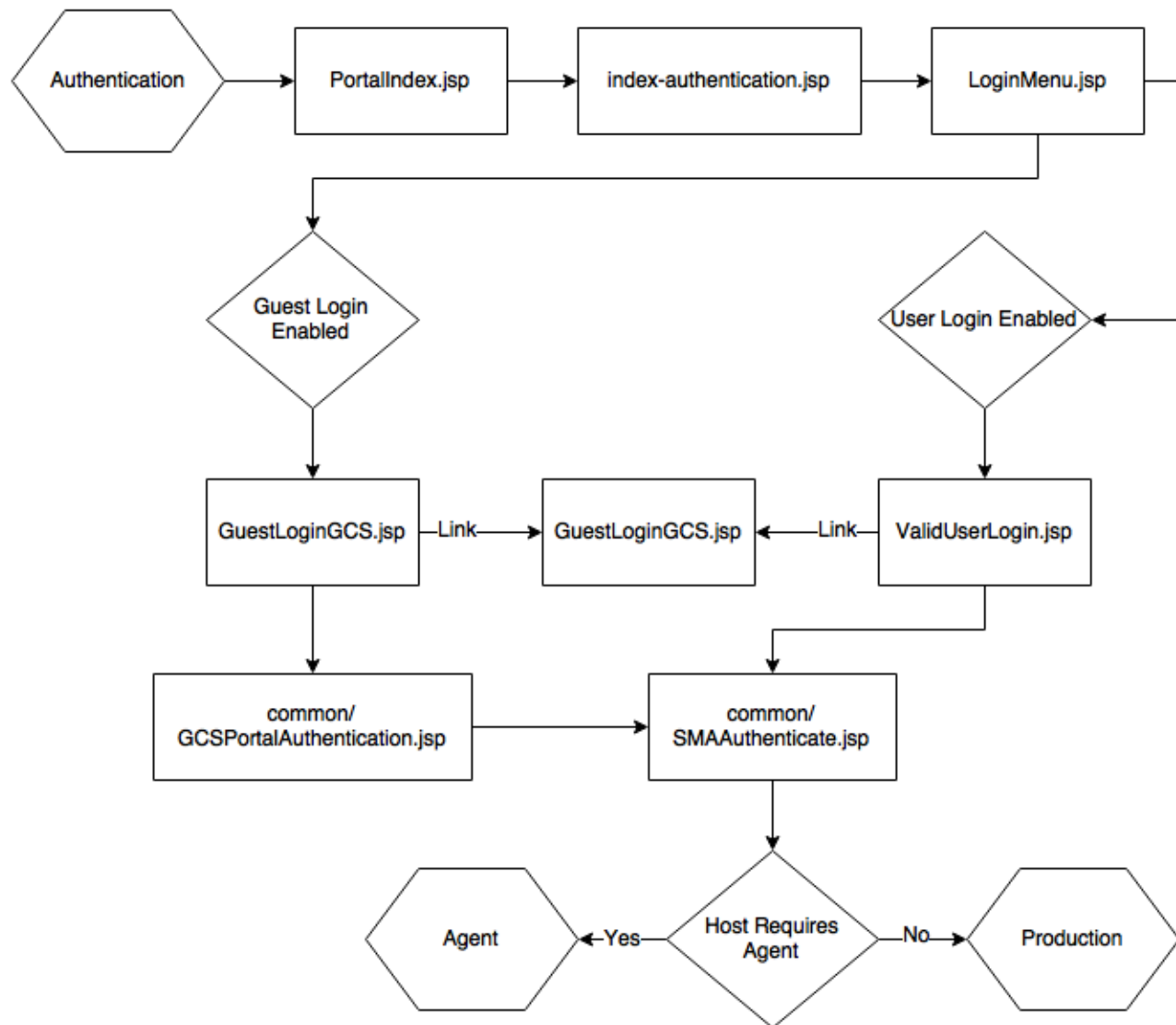
Workflow

When a host connects to the network FortiNAC assesses the host state and determines where to send that host. Below are a series of diagrams that outline the portal pages used when processing a host request for access to the network. These diagrams and pages correspond roughly to the options in the tree on the Portal Configuration Content Editor when using Portal Version 2 web pages. Diagrams of the pages used include the following:

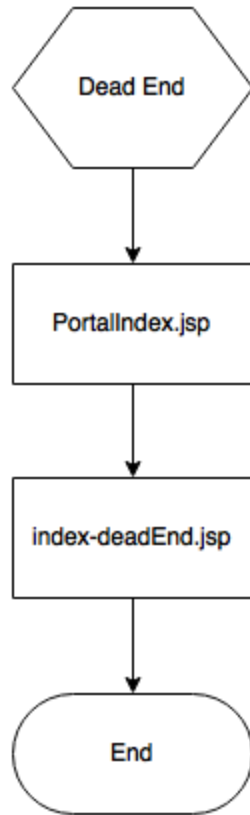
- Registration
- Remediation
- Authentication
- Dead end
- Hub
- VPN
- Agent
- Host inventory

Registration

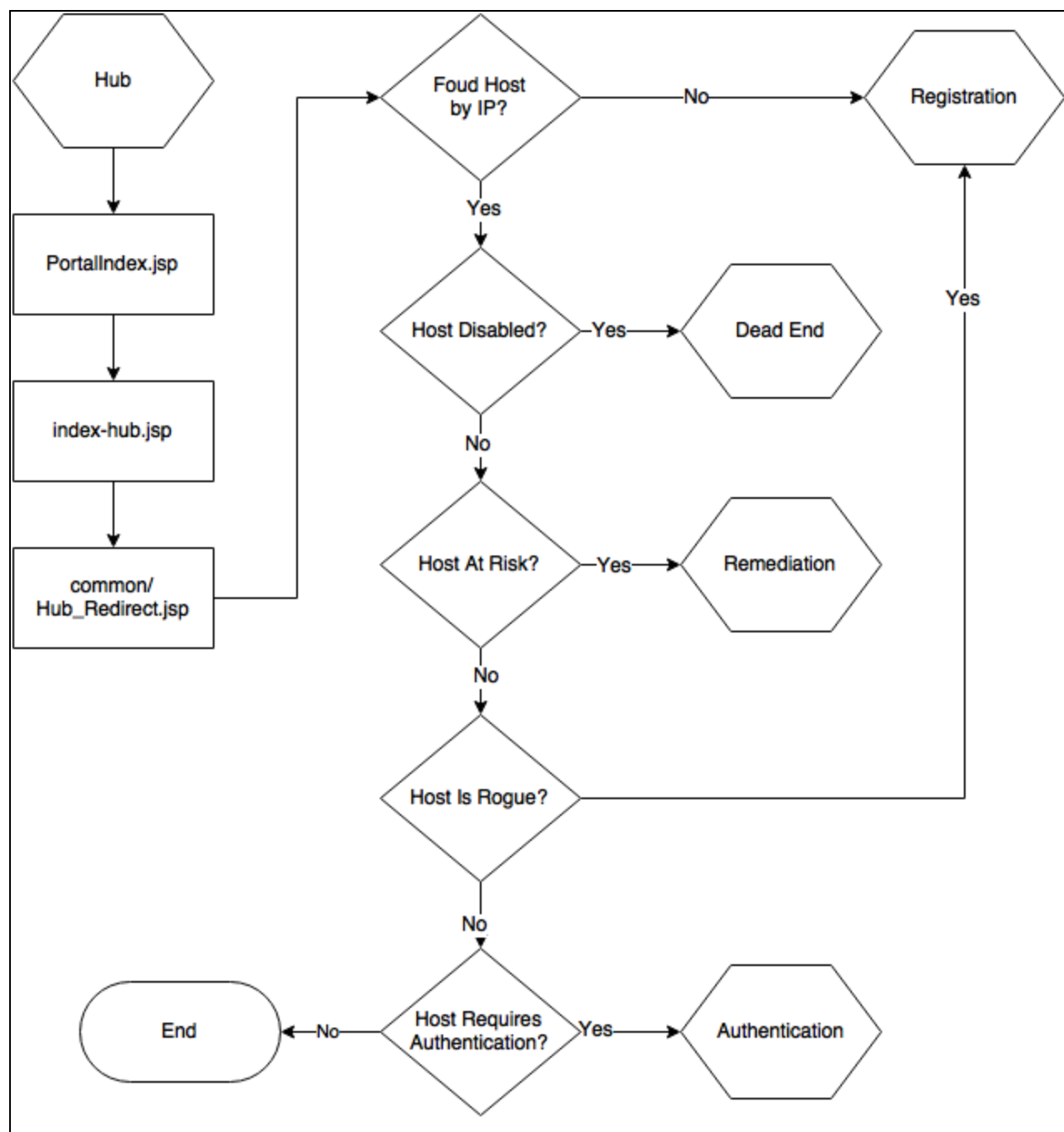
Remediation

Authentication

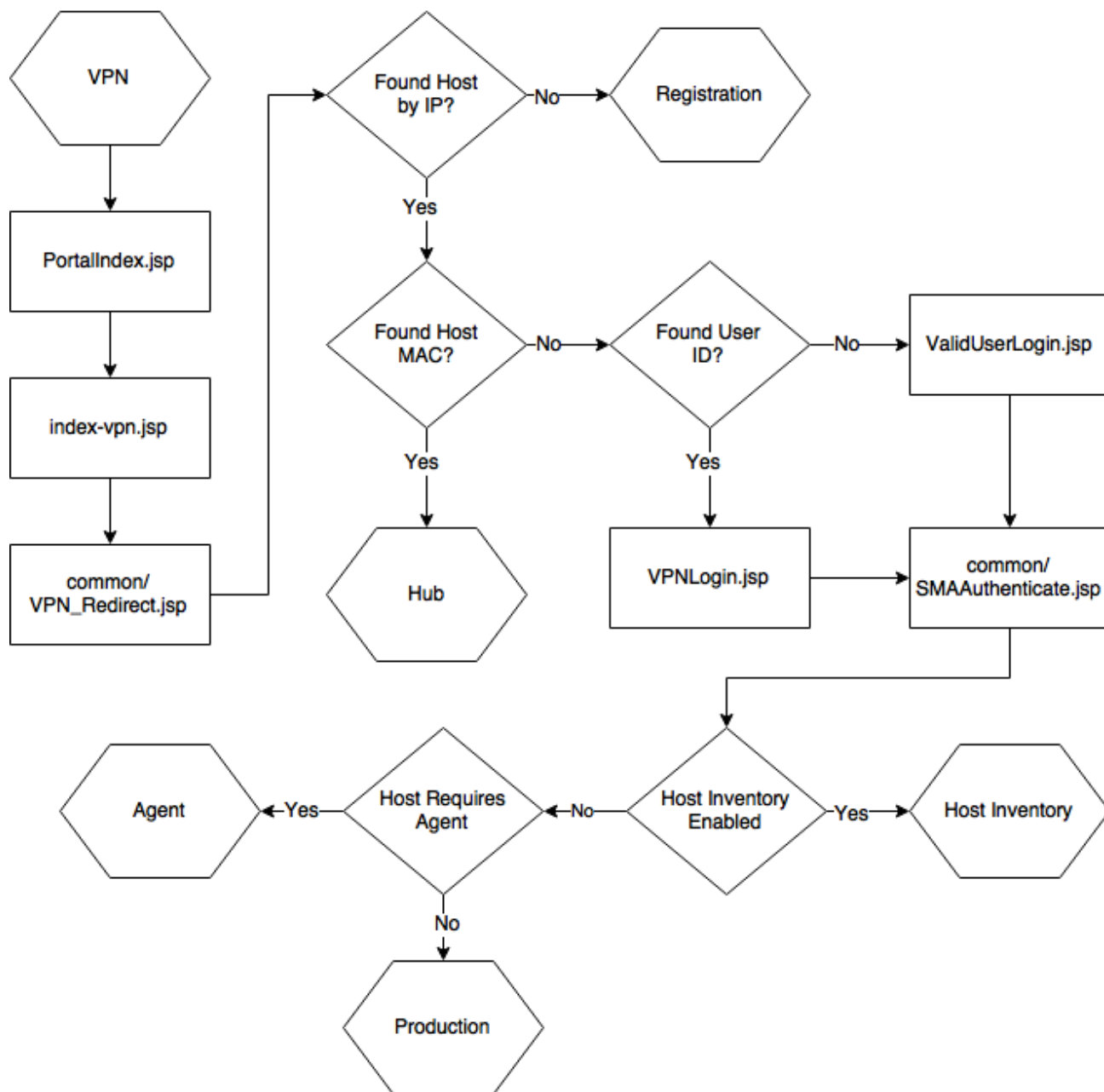
Dead end



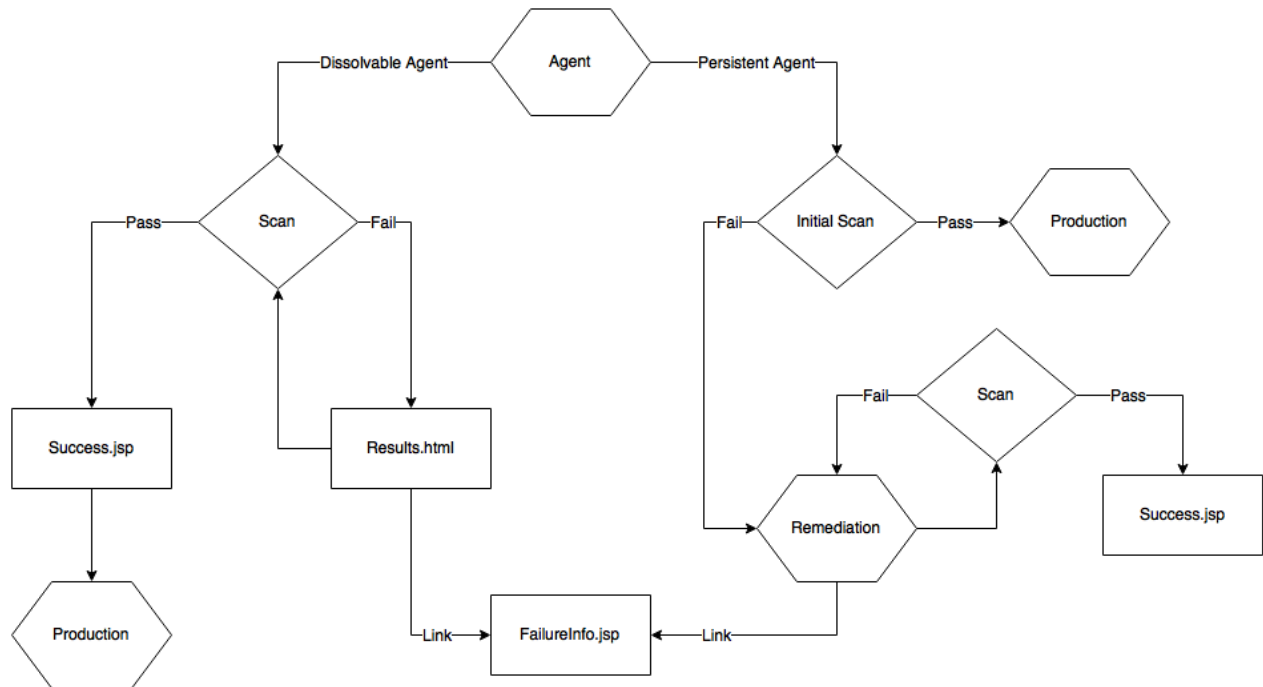
Hub



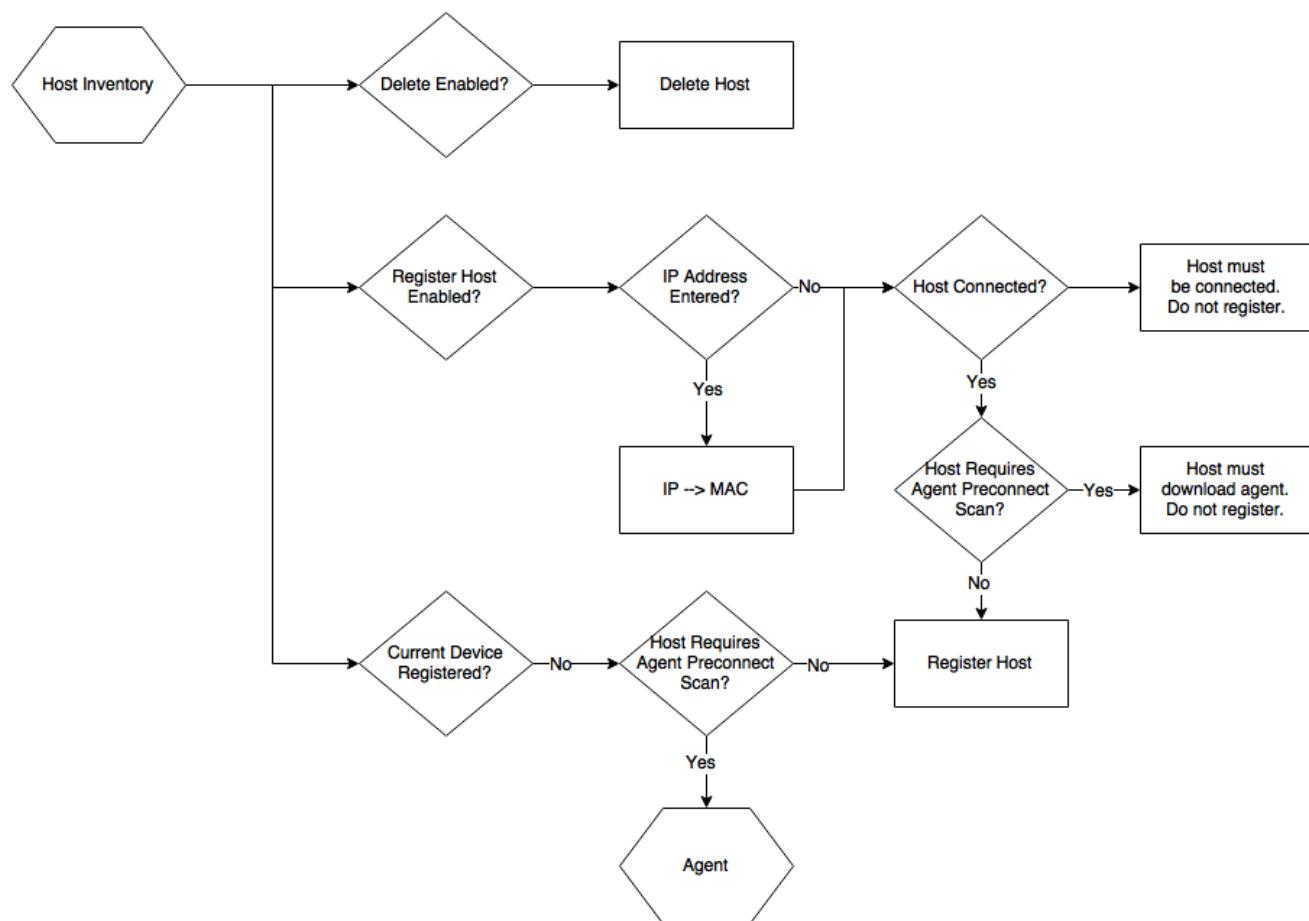
VPN



Agent



Host inventory



Host Inventory

Host inventory provides a way for end-users to manage which of their hosts are registered on the network without requiring assistance from an administrator. This is useful when there is a limit on the number of hosts that each user can have simultaneously registered.

Users are able to register a new host, delete the currently registered host, and log out from a host.

Host Inventory needs to be enabled in Portal Configuration. Then Delete and Logout function also needs to be enabled in Host Inventory Controls in order to manage hosts.

Enable Host Inventory

1. Go to **Portal > Portal Configuration**, and **Portal** and click **Edit**.
2. Go to **Configuration** tab, and select **Portal Pages**.
3. Under **Isolation** section, enable **Host Inventory**. Now Host Inventory page can be found in **Global** configuration tab.

FortiNAC

Dashboard > Users & Hosts > Network > Policy & Objects > Portal > Portal Configuration > Request Processing Rules > Portal SSL > Logs > System

Edit Portal

Name > Styles > Configuration

Portal Pages > Global > Isolation > Registration > Authentication > Remediation > Dead End > VPN > Agent > EasyConnect

Global

Pages/Sections	Display Options
Success Page Type	Default
Show Acceptable Use Policy Before Registration ?	☐
MDM Registration ?	☐

Isolation

Pages/Sections	Display Options
Portal Selector	☒
Host Inventory	☒

4. Go back to **Configuration** tab, and select **Global**.

5. Go to **Host Inventory > Controls**, and enable **Delete Enabled** and **Logout Enabled**.

Users & Hosts > Network > Policy & Objects > Portal > Portal Configuration > Request Processing Rules > Portal SSL > Logs > System

Name > Styles > Configuration

Portal Pages > Global > Isolation > Registration > Authentication > Remediation > Dead End > VPN > Agent > EasyConnect

Common > Global Properties > Host Inventory > Common > Controls > Status Messages > Policy Failure > Apple CNA Instructions

hosts logged limit, please delete other

Hosts Logged Limit Removed ? Click Host Logon button to continue.

☒ Show Registration Counts

Host Registered Count Text ? Hosts Registered

☒ Register Enabled

Remote Host Role ? NAC-Default

Require Valid Vendor OUI ? ☒

Register Host Text ? Register Another Host

Register Dialog Title ? Register Host

Physical Address Label ? MAC Address

Physical Address Example ? e.g. AA:BB:CC:11:22:33

IP Address Label ? IP Address

IP Address Example ? e.g. 192.168.10.10

☒ Delete Enabled

Delete Text ? Delete

Delete Confirmation ? Are you sure you would like to delete this hc

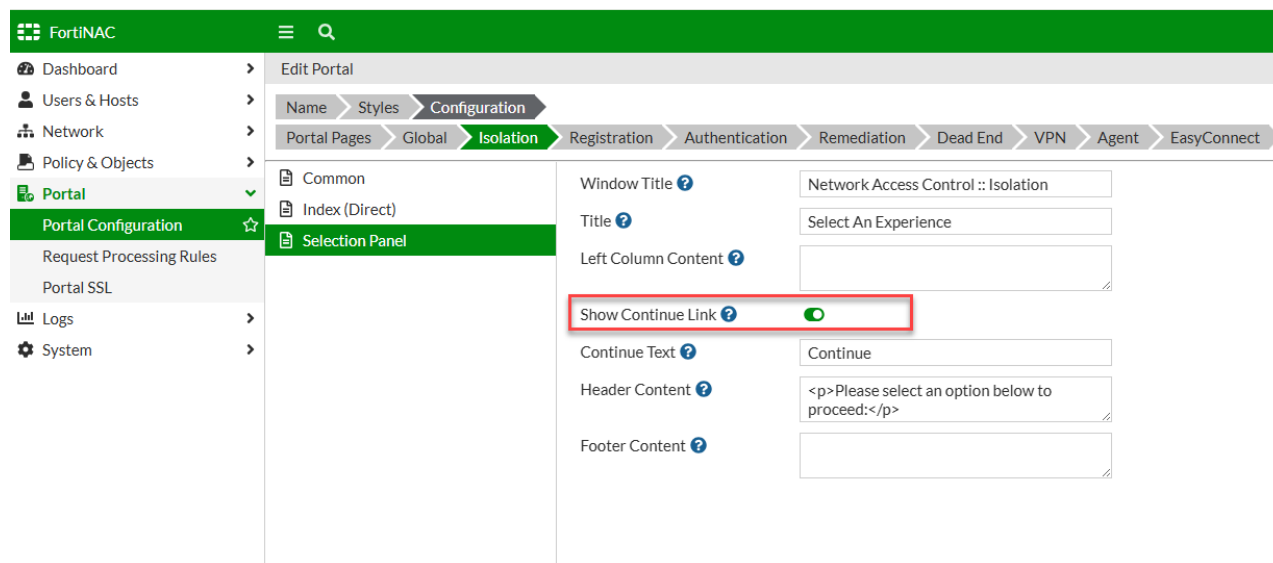
☒ Logout Enabled

Logout Text ? Logout

Logout Confirmation ? Are you sure you would like to logout this hc

6. Go back to **Configuration** tab, and select **Isolation**.

7. Click on **Selection Panel**, and enable **Show Continue Link** to allow user to have the option to continue with existing host access.



8. Click **Save** and now Host Inventory is accessible in the portal page.

Now **Host Inventory** option will become accessible for user in **Captive Portal** Window.



After user authenticates with credentials, the host inventory page will appear with these functions:

- Delete host
- Log out from a host.
- Register the current host that is not registered yet.

- Register another host.
- Log out of the host inventory page.

Portal Selector

Portal Selector allows multiple portal selection when user access Captive Portal page. Multiple Portal Selection allows customized registration options for different groups within an organization.

Enable Portal Selector

1. Go to **Portal > Portal Configuration**, and **Portal** and click **Edit**.
2. Go to **Configuration** tab, and select **Portal Pages**.
3. Under **Isolation** section, enable **Portal Selector**. Now Selection panel and portal Selector can be configured.

The screenshot shows the FortiNAC configuration interface. The left sidebar contains the navigation menu with 'Portal Configuration' selected. The main content area shows the 'Edit Portal' configuration page. The 'Configuration' tab is active, and the 'Portal Pages' sub-tab is selected. Under the 'Isolation' section, the 'Portal Selector' option is highlighted with a red box, and its status is 'On' (indicated by a green toggle switch).

Pages/Sections	Display Options
Success Page Type	Default
Show Acceptable Use Policy Before Registration ?	☐
MDM Registration ?	☐

Pages/Sections	Display Options
Portal Selector	☒
Host Inventory	☒

4. Go back to **Configuration** tab, and select **Isolation**.
5. Go to **Selection** Panel, and edit the contents as well as enable **Continue** link so user can use existing portal to proceed with host registration.

FortiNAC

Dashboard > Users & Hosts > Network > Policy & Objects > **Portal** > Portal Configuration > Request Processing Rules > Portal SSL > Logs > System

Edit Portal

Name > Styles > **Configuration**

Portal Pages > Global > **Isolation** > Registration > Authentication > Remediation > Dead End > VPN > Agent > EasyConnect

Common

Index (Direct)

Selection Panel

Portal Selector

Window Title ? Network Access Control :: Isolation

Title ? Select An Experience

Left Column Content ?

Show Continue Link ? ☒

Continue Text ? Continue

Header Content ? <p>Please select an option below to proceed:</p>

Footer Content ?

6. Click on **Portal Selector**, and select which portal configuration to be enabled in portal selector page.

FortiNAC

Dashboard > Users & Hosts > Network > Policy & Objects > **Portal** > Portal Configuration > Request Processing Rules > Portal SSL > Logs > System

Edit Portal

Name > Styles > **Configuration**

Portal Pages > Global > **Isolation** > Registration > Authentication > Remediation > Dead End > VPN > Agent > EasyConnect

Common

Index (Direct)

Selection Panel

Portal Selector

Portal Options

Portal Option ? ☒ RegistrationPortal ☒ RestrictedPortal

7.

8. Click **Save** to finish.

If you have both **Host Inventory** and **Portal Selector** enabled, **Captive Portal** Window will have these options.

Import portal content

This option allows you to import portal page configuration information. The configuration must have been created using the Content Editor in the Portal Configuration window and exported from that window. Legacy page information configured outside the Content Editor cannot be imported.

When the Portal Page configuration is exported the export file contains portal page properties, style sheets and images combined into a single XML file. The XML file is then added to a zip file created by the export process called PortalContents.zip. Make sure this file is available before you begin the import process.

If you have created multiple portals, each individual portal and its contents are stored as a separate XML file inside the PortalContents.zip. The original shipping portal is stored as portalContents.XML inside the PortalContents.zip. To import only selected portals, delete the XML files for the unwanted portals from the .zip file.

1. Select **Portal > Portal Configuration**.
2. Click on the **Content Editor** tab.
3. Click the **Import** button.
4. On the Import window click the browse button to select the file.
5. Click **OK** to begin importing.
6. When the process is complete a message is displayed indicating that the import was successful.

Export portal content

This option allows you to export the configuration of your portal pages done with the Portal Configuration Content Editor. Legacy page information configured outside the editor cannot be exported. Export to create a backup of your portal page configuration or to copy the configuration to another appliance using the import option. All portal page properties, style sheets and images are included in the export. The export process creates a single file named PortalContents.zip that contains an XML file with the contents of the portal.

If you have created multiple portals, each individual portal and its contents are stored as a separate XML file inside the PortalContents.zip. The original shipping portal is stored as portalContents.XML inside the PortalContents.zip. To import only selected portals, delete the XML files for the unwanted portals from the .zip file.

1. Select **Portal > Portal Configuration**.
2. Click on the **Content Editor** tab.
3. Click the **Export** button.
4. A message is displayed indicating that unsaved changes will not be exported. If you have saved all of your changes, click **Yes** to continue.
5. Depending on the browser you are using you may see slightly different options. Choose **Save**.

Using special characters

In FortiNAC Portal Version 2, there are times when you may need to include special characters in your content that may not exist on your keyboard or may not display properly when copying and pasting. In those cases, you can use the following chart and replace those characters with the HTML entity name or the HTML entity number. See the examples below:

1. Entering the following in the Content Editor:

```
L&#39;acc&egrave;s au pr&eacute;sent syst&egrave;me est r&eacute;serv&eacute; aux utilisateurs autoris&eacute;s de la Banque. Toute activit&eacute; dans ce syst&egrave;me peut &ecirc;tre enregistr&eacute;e et surveill&eacute;e. Conform&eacute;ment &agrave; la politique de la Banque, il est interdit aux utilisateurs de faire un usage inappropri&eacute; ou non autoris&eacute; du syst&egrave;me. Un tel acte peut &ecirc;tre passible de sanctions. En utilisant le syst&egrave;me, vous reconnaissez avoir lu et compris le pr&eacute;sent avis et acceptez de le respecter.
```

2. Will render the following in the Captive Portal:

L'accès au présent système est réservé aux utilisateurs autorisés de la Banque. Toute activité dans ce système peut être enregistrée et surveillée. Conformément à la politique de la Banque, il est interdit aux utilisateurs de faire un usage inapproprié ou non autorisé du système. Un tel acte peut être passible de sanctions. En utilisant le système, vous reconnaissez avoir lu et compris le présent avis et acceptez de le respecter.

ISO-8859-1

- ISO-8859-1 is the default character set in most browsers.
- The first 128 characters of ISO-8859-1 is the original ASCII character-set (the numbers from 0-9, the uppercase and lowercase English alphabet, and some special characters).
- The higher part of ISO-8859-1 (codes from 160-255) contains the characters used in Western European countries and some commonly used special characters.
- Entities are used to implement reserved characters or to express characters that cannot easily be entered with the keyboard.

Reserved characters in HTML

Some characters are reserved in HTML and XHTML. For example, you cannot use the greater than or less than signs within your text because the browser could mistake them for markup.

Entity names are case sensitive.

HTML and XHTML processors must support the five special characters listed in the table below:

Character	Entity number	Entity name	Description
"	"	"	quotation mark
'	'	' (does not work in IE)	apostrophe
&	&	&	ampersand
<	<	<	less-than
>	>	>	greater-than

ISO 8859-1 symbols

Character	Entity number	Entity name	Description
	 	 	non-breaking space
¡	¡	¡	inverted exclamation mark
¢	¢	¢	cent
£	£	£	pound
¤	¤	¤	currency
¥	¥	¥	yen
	¦	¦	broken vertical bar
§	§	§	section
¨	¨	¨	spacing diaeresis
©	©	©	copyright
ª	ª	ª	feminine ordinal indicator

Character	Entity number	Entity name	Description
«	«	«	angle quotation mark (left)
¬	¬	¬	negation
–	­	­	soft hyphen
®	®	®	registered trademark
—	¯	¯	spacing macron
°	°	°	degree
±	±	±	plus-or-minus
²	²	²	superscript 2
³	³	³	superscript 3
´	´	´	spacing acute
μ	µ	µ	micro
¶	¶	¶	paragraph
·	·	·	middle dot
¸	¸	¸	spacing cedilla
¹	¹	¹	superscript 1
º	º	º	masculine ordinal indicator
»	»	»	angle quotation mark (right)
¼	¼	¼	fraction 1/4
½	½	½	fraction 1/2
¾	¾	¾	fraction 3/4
¿	¿	¿	inverted question mark
×	×	×	multiplication
÷	÷	÷	division

ISO 8859-1 characters

Character	Entity number	Entity name	Description
À	À	À	capital a, grave accent
Á	Á	Á	capital a, acute accent
Â	Â	Â	capital a, circumflex accent
Ã	Ã	Ã	capital a, tilde
Ä	Ä	Ä	capital a, umlaut mark

Character	Entity number	Entity name	Description
À	Å	Å	capital a, ring
Æ	Æ	Æ	capital ae
Ç	Ç	Ç	capital c, cedilla
È	È	È	capital e, grave accent
É	É	É	capital e, acute accent
Ê	Ê	Ê	capital e, circumflex accent
Ë	Ë	Ë	capital e, umlaut mark
Ì	Ì	Ì	capital i, grave accent
Í	Í	Í	capital i, acute accent
Î	Î	Î	capital i, circumflex accent
Ï	Ï	Ï	capital i, umlaut mark
Ð	Ð	Ð	capital eth, Icelandic
Ñ	Ñ	Ñ	capital n, tilde
Ò	Ò	Ò	capital o, grave accent
Ó	Ó	Ó	capital o, acute accent
Ô	Ô	Ô	capital o, circumflex accent
Õ	Õ	Õ	capital o, tilde
Ö	Ö	Ö	capital o, umlaut mark
Ø	Ø	Ø	capital o, slash
Ù	Ù	Ù	capital u, grave accent
Ú	Ú	Ú	capital u, acute accent
Û	Û	Û	capital u, circumflex accent
Ü	Ü	Ü	capital u, umlaut mark
Ý	Ý	Ý	capital y, acute accent
Þ	Þ	Þ	capital THORN, Icelandic
ß	ß	ß	small sharp s, German
à	à	à	small a, grave accent
á	á	á	small a, acute accent
â	â	â	small a, circumflex accent
ã	ã	ã	small a, tilde

Character	Entity number	Entity name	Description
ä	ä	ä	small a, umlaut mark
å	å	å	small a, ring
æ	æ	æ	small æ
ç	ç	ç	small c, cedilla
è	è	è	small e, grave accent
é	é	é	small e, acute accent
ê	ê	ê	small e, circumflex accent
ë	ë	ë	small e, umlaut mark
ì	ì	ì	small i, grave accent
í	í	í	small i, acute accent
î	î	î	small i, circumflex accent
ï	ï	ï	small i, umlaut mark
ð	ð	ð	small eth, Icelandic
ñ	ñ	ñ	small n, tilde
ò	ò	ò	small o, grave accent
ó	ó	ó	small o, acute accent
ô	ô	ô	small o, circumflex accent
õ	õ	õ	small o, tilde
ö	ö	ö	small o, umlaut mark
ø	ø	ø	small o, slash
ù	ù	ù	small u, grave accent
ú	ú	ú	small u, acute accent
û	û	û	small u, circumflex accent
ü	ü	ü	small u, umlaut mark
ý	ý	ý	small y, acute accent
þ	þ	þ	small thorn, Icelandic
ÿ	ÿ	ÿ	small y, umlaut mark

Add/Edit a portal

When you create a new portal configuration the content contains the factory default styles, images and text. New portals can also be created by copying an existing portal to a new name. See [Copy a portal on page 733](#).

Add a portal

1. Select **Portal > Portal Configuration**.
2. Click on the **Content Editor** tab.
3. Click the **Create New** Button. You will be redirected to the "Create Portal" page.
4. Enter a unique name and (optional) description for the portal.
5. Click **Save** to save the changes.
6. Click **Next** and proceed to the style tab, or click **Exit** if you want to do other configurations later. See **Edit style sheet** section of this document for next steps.

Edit a portal

Use this option to change the name and configuration of an existing portal.

1. Select **Portal > Portal Configuration**.
2. Click on the **Content Editor** tab.
3. Select the portal you want to modify and click **edit**. You will be redirected to the **Edit Portal** page.
4. Modify the name and (optional) description of the portal.
5. Click **Save** to save the changes.
6. Click **Next** and proceed to the style tab, or click **Exit** if you want to do other configurations later. See **Edit style sheet** section of this document for next steps.

Edit style sheets

The Style Sheet Editor allows you to modify the look and feel of the portal pages seen by your network users. This editor only modifies portal pages distributed with FortiNAC in version 4.1.1 or higher. Legacy portal pages cannot be edited using this tool. See [Content editor on page 632](#) for additional information.

When the Style Sheet Editor is accessed it displays a sample portal page. This gives you a way to preview your changes as you make them. There are two methods for editing your style sheets.

The first method is to click on an item in the sample page to pop-up a window of options that can be modified.

The second method allows you to enter custom rules for different items in the sample page. This option requires knowledge about cascading style sheets and elements within those style sheets.

Some mobile devices may automatically interpret any text resembling a phone number as a hyperlink. As a result, all rules relative to hyperlinks, including text color, are applied and may cause unexpected results. You may need to supply custom rules in the Style Editor to correct any unexpected issues.

Modifying styles using the sample portal page

1. Select **Portal > Portal Configuration**.
2. Click on the **Content Editor** tab.
3. Select the portal you want to modify and click **edit**.
4. Select **Styles** tab.
5. As you pass the mouse over the page, a hand is displayed for items that can be edited.
For example, if you pass the mouse over the word **Registration** on the right side of the window, a hand is displayed and you may see a blue block that reads "editable". Click on the word **Registration** to open a properties window. Options contained within the window will vary depending on the item selected.
6. Make changes as needed and click **Preview** to return to the Style Editor. Your changes display on the sample

portal page.

- When all of the necessary changes have been made, click the **Save** button.

Modify styles using the custom rules definitions



In order to use custom rules, you must have a working knowledge of CSS.

- Select **Portal > Portal Configuration**.
- Click on the **Content Editor** tab.
- If you have created more than one portal, select the portal to be edited from the drop-down list at the bottom of the view.
- In the tree on the left, select **Global > Styles** to display the style editor.
- Scroll to the **Custom Rules Definitions** section at the bottom of the window. Using the Custom Rules option you can add multiple rules and each rule can contain multiple properties.
- To add a rule, click in the field and enter the selector and name of the element you wish to configure. The selector indicates the type of element being modified. For example a period (.) indicates that you are adding a property to a class in the style sheet. In the screen shot shown above, .pagetitle represents the banner at the top of the sample window.
- Click in the **Property** field and enter the name of the property you wish to set. In the example above, the color property is being set.
- Click in the **Value** field and enter the value of the property, such as blue for color or bold for font-weight.
- To add another property to the rule, click the **Add Property** button and an addition set of fields is displayed.
- To add another rule, click the **Add Rule** button and a new rule section is displayed.
- The **Preview** button allows you to see your changes on the sample page.
- The **Reset** button discards all changes and returns the sample page and the custom rules to the state they were in when the Style Editor was first opened.
- To save, click **Apply** at the bottom of the Content Editor View. This saves changes both in the rules section and in the sample page section.

Configuration

The Content Editor allows you to modify the content of the portal pages seen by your network users. This editor only modifies portal pages distributed with FortiNAC in version 4.1.1 or higher. Legacy portal pages cannot be edited using this tool. See [Content editor on page 632](#) for additional information.

If you are familiar with HTML, you can add formatting within the content fields for your pages. Test each page carefully because your formatting may conflict with something that is in the default settings for the page. Make sure to test portal pages in a separate browser of a different brand. If you test in the same browser you will be logged out of the Admin user interface. For example, if you are running the Admin user interface in Google Chrome, test the portal pages in Internet Explorer.

- Select **Portal > Portal Configuration**.
- Click on the **Content Editor** tab.
- Select the portal you want to modify and click **edit**. You will be redirected to the **Edit Portal** page.
- Select the **Configuration** tag.

5. Modify the properties as needed and click **Apply** to save your changes. When changes are made to the portal pages there is a delay before the changes are displayed.

Field types on each page include the following:

Type	Description
Boolean	Check box that enables or disables a feature or subsequent field.
Text	Text fields are available for you to enter custom text that is displayed on your Captive Portal Page. If you are familiar with HTML, you can include HTML in these fields. For example, to make something bold and italics, you would do the following: <pre><i>Contact the Help Desk.</i></pre> The message on the web page would display as: <i>Contact the Help Desk.</i> For users who are accessing your web pages you may also have text fields. These fields are set to type Input and typically only allow text.
Input	If you have set a data entry field to type input, you are indicating that the web page user should enter text. You can enter a default value to prompt the user but it can be overridden. For example, if you set Postal Code to your local postal code, most users would not have to modify this field and it would save them a step.
Password	If you have set a data entry field to type password, any data typed into the field by the user will display as dots or asterisks to mask the actual characters being entered.
Hidden	If you have set a data entry field to type hidden, the user does not see it on the web page; however, it does contain data that is passed to the server. You must enter the data in the Portal Content Editor. For example, if all users who register via the Registration page should be set to a particular Role, such as Staff, you can enter Staff in the Role field for them and mark it as hidden.
Select	If you have set a data entry field to type select, the user is presented with a drop-down list of options on the web page. To construct the list of options you must enter list items as follows: (Value,Name : Value,Name) Example: Color1,Blue : Color2,Red : Color3,Green
Inline Help icon	Displays inline help containing a description and usage for the field.



Text fields in the Portal Contents Editor accept HTML. However, if you copy and paste HTML developed in another program you may corrupt the data stored for your web pages. Specifically, HTML containing curly or curved quotes instead of straight quotes will corrupt your web pages and they will become unusable.

Portal Pages

An at-a-glance overview of the different configuration methods. For more details, see the pages of the admin guide that refer to the individual sections.

Settings

Setting	Definition
Global	
Success Page Type	Select whether the host should be redirected to the default Success page or the Host Inventory Success page after logging in within the Registration or VPN context.
Show Usage Policy Before Registration	If enabled, displays the Usage Policy to the user before registration. Usage Policy text is entered in the Content Editor under Registration-Usage Policy-Usage Policy Content.
MDM Registration	If enabled, all browsers with mobile user agents will be redirected to the MDM Registration page. MDM settings are located under Registration > MDM Registration.
Isolation	
Portal Selector	Displays a portal selection page immediately following isolation. Users can pick a portal from the list to continue the portal process.
Registration	
Standard User Login	If enabled, the Standard login option appears in the login menu for regular network users. Instructions: Select whether instructions will be included in this page, as a link to Instructions, or not at all. Instruction are entered in the Content Editor under Registration-Instructions. The Registration > Instruction page will be available if and only if instruction is set to not "none" for at least one of the registration portal pages. Registrations Require Approval: Can be configured to either: • An Administrator with Self Registration Request Permissions • Any Administrator that belongs to a specified User group Administrators that belong to the group will be able to approve, regardless of their permissions. Administrators that do not belong to that group will be unable to approve. The Standard User Registration Approval setting (under Registration > Standard User Login > Standard User Registration Approval) will be available if and only if is set to "An Administrator with Self Registration Request Permissions" or "Any Administrator that belongs to a specified User group"
Guest Login	If enabled, the Guest login option appears in the login menu for regular network users. Instructions: Select whether instructions will be included in this page, as a link to Instructions, or not at all. Instruction are entered in the Content Editor under Registration-Instructions. The Registration > Instruction page will be available if and only if instruction is set to not "none" for at least one of the registration portal pages. Registrations Require Approval: Can be configured to either: - An Administrator with Self Registration Request Permissions

Setting	Definition
	- Any Administrator that belongs to a specified User group Administrators that belong to the group will be able to approve, regardless of their permissions. Administrators that do not belong to that group will be unable to approve. The Guest User Registration Approval setting (under Registration > Guest Login > Guest User Registration Approval) will be available if and only if is set to "An Administrator with Self Registration Request Permissions" or "Any Administrator that belongs to a specified User group"
Self-Registration Guest Login	If enabled, the Self registration guest login option appears in the login menu for regular network users. Instructions: Select whether instructions will be included in this page, as a link to Instructions, or not at all. Instruction are entered in the Content Editor under Registration-Instructions. The Registration > Instruction page will be available if and only if instruction is set to not "none" for at least one of the registration portal pages.
Anonymous Authentication	If enabled, the Anonymous Authentication option appears in the login menu.
Game Console Registration	If enabled, the Game Console Registration option appears in the login menu.
Custom Login	If enabled, the Standard login option appears in the login menu for regular network users. Instructions: Select whether instructions will be included in this page, as a link to Instructions, or not at all. Instruction are entered in the Content Editor under Registration-Instructions. The Registration > Instruction page will be available if and only if instruction is set to not "none" for at least one of the registration portal pages. Registrations Require Approval: Can be configured to either: - An Administrator with Self Registration Request Permissions - Any Administrator that belongs to a specified User group Administrators that belong to the group will be able to approve, regardless of their permissions. Administrators that do not belong to that group will be unable to approve. The Custom User Registration Approval setting (under Registration > Custom Login > Custom User Registration Approval) will be available if and only if is set to "An Administrator with Self Registration Request Permissions" or "Any Administrator that belongs to a specified User group"
Authentication	
Standard User Login	When enabled, the Standard login option appears in the login menu.
Guest Login	When enabled, the Guest Login option appears in the login menu.
Request New Credentials	When enabled, the New Credentials option appears in the login menu.
Custom Login	If enabled, the Custom Registration Option appears in the login menu.
VPN	

Setting	Definition
Download Page Instructions	Select whether instructions will be included in this page, as a link to Instructions, or not at all. Instruction are entered in the content editor under VPN > instructions.
User Login Instructions	Select whether instructions will be included in this page, as a link to Instructions, or not at all. Instruction are entered in the content editor under VPN > instructions.

Global

Global properties are common to all portal pages. These properties are organized into property groups. Select a property group to view or modify property settings.

Settings

Setting	Definition
Network Label	Text label for the left side of the banner on each portal page.
Show Passed Tests	Display criteria that were met during a host scan.
Show Left Column	Display a column to the left of the main content.
Standard User Login Type	Select the authentication method for the Standard User Login page. This field must match the field selected in Persistent Agent Properties under the Credential Configuration Tab. For more information about login types, see Configure authentication credentials .
Custom Login Type	Select the authentication method for the Custom Login page. For more information about login types, see Configure authentication credentials .
Game Console Registration Login Type	Select the authentication method for the Game Console Registration page. For more information about login types, see Configure authentication credentials .
Authenticate Standard Users	If enabled, this option authenticates and registers users at the same time. Prevents users from needing to enter credentials on both the Registration and Authentication pages.
Enable Mobile Enhancements	If enabled, uses an override stylesheet to optimize the portal for modern mobile browsers on mobile devices running Apple iOS, Android, Symbian, and others.
Use JavaScript UI Enhancements	If enabled, allows the system to use user interface enhancements such as the accordion view in all instructions pages. Features using JavaScript Enhancements can be disabled individually.
Use Configured MDM	If enabled, all browsers with mobile user agents will be redirected to the MDM Registration page.

Setting	Definition
Success Page Type	Select whether the host should be redirected to the default Success page or the Host Inventory Success page after logging in within the Registration or VPN context.
Enable xxx Auth	If enabled, allows social media authentication for captive portal set up. See social media for captive portal .
Social Media for Captive Portal	 Related documentation See the FortiNAC Captive Portal Azure AD Authentication guide. FortiNAC is able to use various social media sites for authenticating users via the captive portal. Currently supported sites: • Facebook • Google • LinkedIn • Outlook • Azure AD • Twitter • Yahoo Using the social media site's developer account, an app can be created that will provide an "App ID" or "Client ID" and a "Secret". These values are then entered in the Portal > Portal Configuration > Global > Settings. One of the pages in the captive portal is then configured for Social Networking authentication. When a user selects the link for Social Networking in the captive portal, the Social Media Networks are displayed for them to choose. Once the user properly authenticates with their Social Media Account, normal processing of the captive portal occurs. General Steps: 1. Log into the developers site of the social media network you wish to configure. Create and set up an app for the site and save the Client ID and Client Secret. Use https://fortinac02.classicnetworking.net/registration/CustomLogin.jsp as the authorized redirect URL. 2. In FortiNAC, navigate to Portal > Portal Configuration > Global > Settings. Change either Standard, Custom, or Game Login type to Social. 3. Check the box for the Social Media Network Auth to enable its configuration. Input the Client ID and Client Secret. 4. Click Apply. 5. Navigate to Portal > Portal Configuration > Registration > Login Menu 6. Edit the Login Type that was chosen with the desired text 7. Click Apply to save 8. Navigate to Portal > Portal Configuration > Registration > (Login Type) Login 9. Edit the text as desired

Setting	Definition
	10. Click Apply to save.

Common text

Setting	Definition
Username Label	Text label displayed on all generic Username fields.
Password	Text label displayed on all generic Password fields.
Footer Text	Text displayed at the bottom of each page in the footer section.
Physical Address	Text label displayed on fields where users enter the Physical Address or MAC Address of their host, gaming device or other network device.
IP address	Text label for the IP address field where users enter the IP address of their host.
Instructions	Text for all links to instructions, such as Persistent Agent installation instructions.
Result	Text label displayed above the result panel.
Passed Tests	Text label displayed above the list of criteria that was met during a host scan.
Passed Tests Help	Help information displayed above the list of criteria that was met during a host scan.
Warnings	Text label displayed above the list of criteria that generated warnings during a host scan. Warnings do not stop the user from accessing the network.
Warnings Help	Help information displayed above the list of criteria that generated warnings during a host scan.
Failed Tests	Text displayed above the list of criteria that was not met during a host scan.
Failed Tests Help	Help information displayed above the list of criteria that was not met during a host scan.
Default Select Option Text	Text label displayed above any selection boxes if they are enabled on a form.
Registration	Text label displayed on the banner for Registration.
Login Button Text	Text displayed on all Login buttons.
Logout	Text displayed on all Logout buttons.
Back	Text displayed on all Back buttons.
Register	Text displayed on all Register buttons. User clicks Register when registration information is complete.
Reset	Text displayed on all Reset buttons.
Agree	Button text for Agree
Disagree	Button text for Disagree
Failed Scan	Message displayed when a persistent agent client failed tests during a rescan.

Error messages

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Heading	Text label displayed on the banner when there is an error.
Left Column Content	Error message displayed when there is an error processing input in the left column of any page.
Unsupported OS	Error message displayed when a host has an unsupported operating system and the Security Policy used to scan that host has the unsupported operating system agent option set to "None-Deny Access".
Jailbroken Device Failure	Error message displayed when a host exceeds the threshold configured for potentially jailbroken devices.
Unauthorized Mobile Agent Failure	Error message displayed when an unauthorized host attempts to register using the Mobile Agent.
Host Already Registered	Error message displayed when the host is already registered.
User Account is invalid or disabled	Customizable message displayed when the user is not found. Defaults to "Authentication Failure".
Invalid Registration Key	Uncommon error message displayed when the system was unable to register the host with the supplied authentication key.
Other Registration Error	Error message displayed when any other Registration error occurs. Note: An additional error message is displayed after this text, which typically starts with "Registration Failed:".
Invalid OUI	Error message displayed when the Vendor OUI of the Physical Address entered is not configured as a gaming device OUI. To configure additional Vendor OUIs select Go- Manage - Vendor OUIs.
Gaming Device Not Connected	Error message displayed when the Gaming Device was not connected to the network before the registration attempt.
Host Not Found	Error message displayed when the software cannot locate the host attempting to use the portal.
Agent Version/Filename Does Not Exist	Error message displayed when a user tries to download an agent and that request references an agent that does not exist or has incomplete file information.
Isolation Redirect Error	Error message displayed when the host is still isolated because it could not be redirected. No action is required for the user. However, this does require network configuration changes.
No Scan Failures	Error message displayed when a host is in the remediation network but the host is not marked as failed for any scans.
Unable to Rescan	Error message displayed when a host is in the remediation network and tries to rescan, but the server was unable to scan via the agent.
General Error	Error message displayed for unknown or unspecified errors.

Failure information settings

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the Failure Information page.
Left Column Content	Text displayed in the left column of the page.
Rescan Button Text	Text displayed in a button on the Failure Information page to allow the user to re-run the failed Vulnerability Scan for their device.
Scan Pending Button Text	Text displayed in the Rescan Button while the scan is pending response. The button will be disabled while the scan is pending.
Vulnerability Scan Passed Test	Content displayed in Failure Information page when the vulnerability scan being viewed has no failures for the current device.
Poll for Vulnerability Rescan Results (minutes)	The frequency with which the Portal queries FortiNAC for updated scan results from the Vulnerability Scanner.

Styles

Setting	Definition
Portal Custom Styles	Contains the CSS text for the portal's custom styles.
Portal Custom Skin	Contains the CSS text for the portal's custom skin, created by the editor.

Social Media for Captive Portal



Related documentation

See the [FortiNAC Captive Portal Azure AD Authentication](#) guide.

How it works:

FortiNAC is able to use various social media sites for authenticating users via the captive portal.

Currently supported sites:

- Facebook
- Google
- LinkedIn
- Outlook
- Azure AD
- Twitter
- Yahoo

Using the social media site's developer account, an app can be created that will provide an "App ID" or "Client ID" and a "Secret". These values are then entered in the **Portal > Portal Configuration > Global > Settings**.

One of the pages in the captive portal is then configured for Social Networking authentication. When a user selects the link for Social Networking in the captive portal, the Social Media Networks are displayed for them to choose. Once the user properly authenticates with their Social Media Account, normal processing of the captive portal occurs.

General Steps:

1. Log into the developers site of the social media network you wish to configure. Create and set up an app for the site and save the Client ID and Client Secret. Use <https://fortinac02.classicnetworking.net/registration/CustomLogin.jsp> as the authorized redirect URL.
2. In FortiNAC, navigate to Portal > Portal Configuration > Global > Settings. Change either Standard, Custom, or Game Login type to **Social**.
3. Check the box for the Social Media Network Auth to enable its configuration. Input the Client ID and Client Secret.
4. Click **Apply**.
5. Navigate to Portal > Portal Configuration > Registration > Login Menu
6. Edit the Login Type that was chosen with the desired text
7. Click **Apply** to save
8. Navigate to Portal > Portal Configuration > Registration > (Login Type) Login
9. Edit the text as desired
10. Click **Apply** to save.

Host inventory

Common

Setting	Definition
Nameless Host Label	Text label for any hosts that do not have a name.
Text Content	Text providing instructions and information about how to use the Host Inventory.
Status Section Title	Text label for the status messages for each host.
Adapters Section Title	Text label for the adapters for each host.
Show Operating System	When enabled, the operating system field is displayed for each host.
Show Notes	When selected, the notes field is displayed for each host in the host list.

Controls

Setting	Definition
Log Out Text	The text displayed on the log out button.
Log out URL	The URL for the landing page where the user will be redirected when the user logs out or when the session times out.
Register This Host	The text of the banner where the user may register their current host.

Setting	Definition
Host Login Text	The text value displayed in the host login button when max logged host limit reached.
Host Logged Count Text	The text displayed after the host count.
Reach Max Hosts Logged	The text value displayed when max logged host limit reached.
Hosts Logged Limit Removed	The text value displayed when max logged hosts limit removed.
Show Registration Counts	When enabled, the user can view the current vs. maximum number of registrations available.
Host Count Text	The text displayed after the ratio of hosts and maximum number of registrations that are allowed.
Register Enabled	When enabled, the user can register new hosts from the host inventory.  In a FortiNAC Manager environment, to add new hosts to a user's Host Inventory the user must access the Host Inventory portal from the FortiNAC Server containing a rogue record for the host being added. Once the host is added, the FortiNAC Manager will enable access for the new registered host on any FortiNAC Server.
Delete Enabled	When enabled, user can delete registered host in host Inventory page, required when using Host Inventory as one of the portal selection.
Logout Enabled	When enabled, user can log out from host inventory page, required when using Host Inventory, required when using Host Inventory as one of the portal selection.
Remote Host Role	The role to apply to guest who register third party hosts through the portal. It does not apply when the host being registered is currently using the portal.
Require Valid Vendor OUI	When enabled, the vender OUI of the MAC address is checked against the known OUIs.
Register Host Text	The text displayed on the register button.
Register Dialog Title	The text displayed as the title of the register dialog.
Physical Address Label	The label text displayed for the physical address.
Physical Address Example	The example value displayed for the physical address.
IP address Label	The label text displayed for the IP address.
IP address Example	Example value displayed for the IP address.
Delete Enabled	When enabled, users can delete their host from the FortiNAC.  Deleting a host locally cannot be done in a FortiNAC Manager enviroment.

Setting	Definition
Delete Text	The text displayed on the Delete button.
Delete Confirmation	The message that is displayed to confirm if the host should be deleted.

Status messages

Setting	Definition
Disconnected	Status message displayed when the host is disconnected and has no other status messages.
Connected	Status message displayed when the host is successfully connected.
Disabled	Status message displayed when the host has been disabled.
Marked as Security Risk	Status message displayed when the host is marked as a security risk.
Passed the Security Scan	Status message displayed when the host has passed the security scan.
Invalid MAC Address	Status message displayed when the host has an invalid MAC address.
User is Logged On	Status message displayed when a user is logged onto the host.
Directory Authentication Disabled	Status message displayed when the directory authentication is disabled.
Not Authenticated	Status message displayed when the host is not authenticated.
Has a Static IP address	Status message displayed when the host has a static IP address.
Has Persistent Agent	Status message displayed when the host has the Persistent Agent.
Connected Through VPN	Status message displayed when the host connected through VPN.
Connected Through Dialup	Status message displayed when the host connected through dial up.
Will Be Scanned On Connect	Status message displayed when the host will be scanned on connect.
Is Being Scanned	Status message displayed when the host is being scanned.
Persistent Agent Connected	Status message displayed when the host has the Persistent Agent and the agent is actively communicating.

Policy failure

Specify the Default Instructions to show when the host fails their Policy. Navigate to **Policy & Objects > Endpoint Compliance > Scans**, select a scan, and then select a category (Operating System, Anti-Virus). Click an operating system or anti-virus package to see the Web Address parameter that is being used.

Default instructions

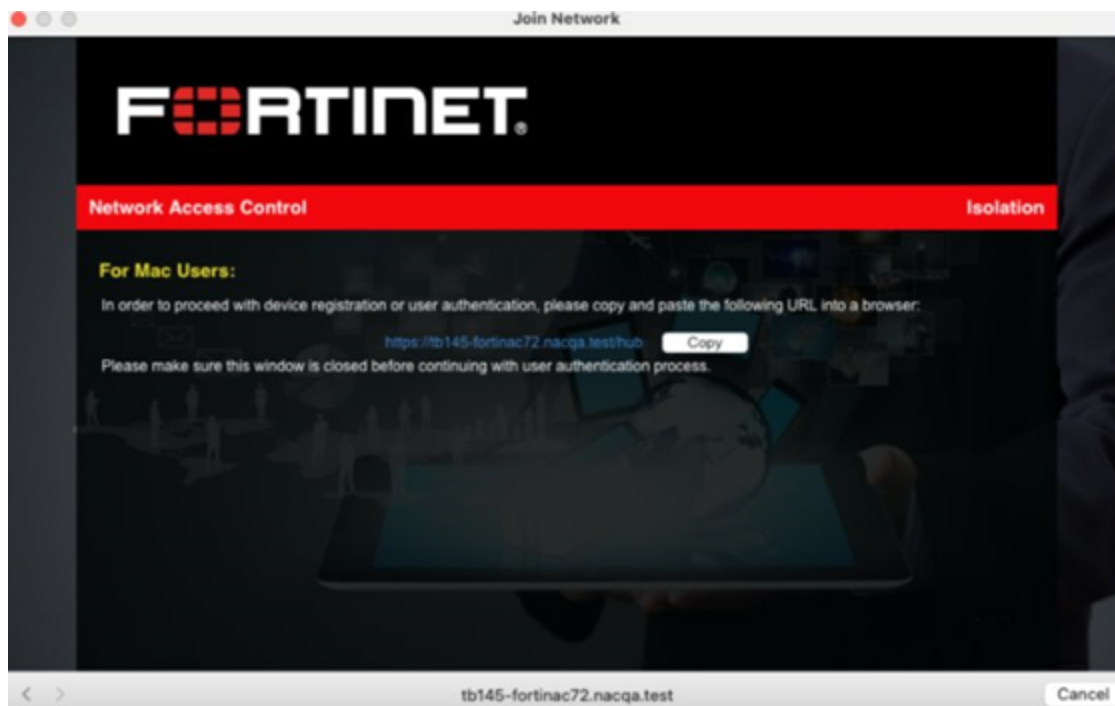
Setting	Definition
Windows Operating System	Displayed when clicking on the link for the Operating System.

Setting	Definition
Windows Operating System Updates	Displayed when clicking on the link for the Windows Service Pack or Updates.
macOS Operating System and Updates	Displayed when clicking on the link for the Operating System or Updates for macOS systems.
Anti-Spyware installed	Displayed when clicking on the link for the Anti-Spyware.
Anti-Spyware Definitions	Displayed when clicking on the link for the Anti-Spyware Definition Products..
Anti-Virus Installed	Displayed when clicking on the link for the antivirus products.
Anti-Virus Definitions	Displayed when clicking on the link for the antivirus Definitions products.

Apple CNA Instructions Portal

The purpose of using Apple CNA Instruction to register the Apple device user is to provide workaround when AppleCNA Captive Portal does not open automatically. AppleCNA Captive Portal opens automatically by default when an Apple device is connected to a hotspot and provide instructions to register.

However, AppleCNA Captive Portal prevents Apple devices from registering host on FortiNAC due to network connection issue. The work around is to enable Auto Configure at **Portal > Request Processing Rules**, then Apple CNA Instruction Portal will automatically appear with instruction to copy and paste the registration URL to a browser to finish host registration.



Default instructions

Setting	Definition
Window Title	Text labeled displayed for the title of the browser window.
Title	Text title for the Apple CAN instructions page.
Left Column Content	Text displayed on the left column of the page.
Top Content	Text providing instructions and information on how to register without using Apple Captive Network Assistant.
Copy Button Text	Button to copy text.
Bottom Content	Text after the portal URL that explains how to reach the portal outside of the CAN.

Isolation

Configure the settings and behavior of your portal pages for hosts in isolation.

Common

Setting	Definition
Context Title	Text label to indicate the functional purpose of the context.

Index (redirect)

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title displayed above the content property contents.
Left Column Content	Text displayed in the left column of the page.
Content	Text describing the redirect.

Portal selector

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.

Setting	Definition
Title	Text title displayed above the content property contents.
Left Column Content	Text displayed in the left column of the page.
Show Continue Link	If enabled, a continue link is shown that allows the user to proceed with the current portal.
Continue Text	Text for the button to proceed with the current portal selection.
Header Content	Text describing the portal options the user can select. This is displayed below the option to continue with the current portal.
Portal Options	A selection of the portals shown in the list of available options
Footer Content	Text to display below the portal selections

Registration

Configure the settings and behavior of your portal pages for registering hosts on your network.

Common text

Setting	Definition
Context Title	Text label to indicate the functional purpose of the context.

Login menu

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text for the title in the body of the login menu page. Displays above the text entered in the Text Content property.
Left Column Content	Text displayed in the left column of the login page.
Text Content	Text providing instructions or requirements for the use of the Login Menu. The Login Menu may contain multiple login options, such as Users or Guests.
Standard Login Enabled	If enabled, the Standard login option appears in the login menu for regular network users.
Standard Login Title	Text label above the link to the regular network user login.
Standard Login Description	Text displayed in the link to the regular network user login.
Standard Login Order	Integer value indicating the order this item should appear in on the page
Guest Login Enabled	If enabled, the Guest Login option appears in the login menu.
Guest Login Title	Text label above the link to the guest login.

Setting	Definition
Guest Login Description	Text displayed in the link to the guest login.
Guest Login Order	Integer value indicating the order this item should appear in on the page
Self Registration Guest Login Enabled	If enabled, the Self Registration Guest Login option appears in the login menu.
Self Registration Guest Login Title	Text label above the link to the self registration guest login.
Self Registration Guest Login Description	Text displayed in the link to the self registration guest login.
Self Registration Guest Login Order	Integer value indicating the order this item should appear in on the page.
Anonymous Authentication Enabled	If enabled, the Anonymous Authentication option appears in the login menu.
Anonymous Authentication Title	Text label above the link to the anonymous authentication.
Anonymous Authentication Description	Text displayed in the link to the anonymous authentication.
Anonymous Authentication Order	Integer value indicating the order this item should appear in on the page
Game Console Registration Enabled	If enabled, the Game Console Registration option appears in the login menu.
Game Console Title	Text label above the link to the Game Console Registration.
Game Console Description	Text displayed in the link for the Game Console Registration.
Game Console Order	Integer value indicating the order this item should appear in on the page
Custom Registration Enabled	If enabled, the Custom Registration Option appears in the login menu.
Custom Registration Title	Text label above the link to the custom registration.
Custom Registration Description	Text displayed in the link for a custom device registration, such as a mobile device.
Custom Registration Order	Integer value indicating the order this item should appear in on the page.

Standard user login

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the first paragraph in the login page. Displays above the text entered in the Introduction property.
Left Column Content	Text displayed in the left column of the page.

Setting	Definition
Introduction	Text displayed in the first paragraph of the regular network user login page.
Secondary Text	Text displayed in the second paragraph of the regular network user login page.

Standard user login form

Setting	Definition
Form Title	Text label displayed at the top of the login form.
Form Action	Redirects the user to the next page in the sequence.  Changing the form action to an unsupported page may affect functionality.
Success Page (Relative)	Relative URL to the success message.  Changing this may affect supported functionality.
Missing Fields Message	Message displayed to the user if all required fields on the form are not completed.
Host Expiration Period Enabled	If enabled, the amount of time that the host can access the network is limited to the time entered in the Host Expiration Period Value field. The Host Expiration Period Value field defaults to hidden. The time value provided by the Administrator and is submitted with the rest of the form data.
Host Expiration Period Unit	The Unit of measurement for the amount of time that the host will be registered before expiry.
Host Expiration Period Value	The amount of time that the host will be registered before expiry.
Username Field Enabled	If enabled, displays a Username field on the form.
Username Field Required	If enabled, the user is required to complete this field on the form.
Username Field Label	Text label for the Username field on the form.
Username Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Username Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.

Setting	Definition
Password Field Enabled	If enabled, displays a password field on the form.
Password Field Required	If enabled, the user is required to complete this field on the form.
Password Field Label	Text label for password field on the form.
Password Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Password Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
First Name Field Enabled	If enabled, displays a First Name field on the form.
First Name Field Required	If enabled, the user is required to complete this field on the form.
First Name Field Label	Text label for the First Name field on the form.
First Name Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
First Name Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Last Name Field Enabled	If enabled, displays a Last Name field on the form.
Last Name Field Required	If enabled, the user is required to complete this field on the form.
Last Name Field Label	Text label for the Last Name field on the form.
Last Name Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Last Name Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Security and Access Value (S&A) Field Enabled	If enabled, displays a field for the Security and Access Value on the form.

Setting	Definition
S&A Field Required	If enabled, the user is required to complete the Address field on the form.
S&A Field Label	Text label for the S&A field on the form.
S&A Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Role Field Enabled	If enabled, network access is limited based on the Role Name in the Role Field Value field and the roles created under Go - Manage - Roles. Roles provide location-based access control.
Role Field Required	If enabled, this field must be completed to submit the form.
Role Field Label	Text label for the Role field on the form.
Role Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Role Field Value	Data entry field used to submit data with the form. Requires a role name. Roles are used to control network access. Typically this field is set by the administrator with the field type set to hidden. Role names must match those in the database. You can also create a list of roles for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green.
Title Field Enabled	If enabled, displays a field for the user's title on the form.
Title Field Required	If enabled, the user is required to complete this field on the form.
Title Field Label	Text label for the title field on the form.
Title Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Title Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Address Field Enabled	If enabled, displays a field for the user's address on the form.
Address Field Required	If enabled, the user is required to complete the Address field on the form.
Address Field Label	Text label for the Address field on the form.

Setting	Definition
Address Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Address Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
City Field Enabled	If enabled, displays a field for the user's city on the form.
City Field Required	If enabled, the user is required to complete this field on the form.
City Field Label	Text label for the City field on the form.
City Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
City Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
State/Province Field Enabled	If enabled, displays a State/Province field on the form.
State/Province Field Required	If enabled, the user is required to complete this field on the form.
State/Province Field Label	Text label for the State/Province field on the form.
State/Province Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
State/Province Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Postal Code Field Enabled	If enabled, displays a Postal Code field on the form.
Postal Code Field Required	If enabled, the user is required to complete this field on the form.
Postal Code Field Label	Text label for the Postal Code field on the form.

Setting	Definition
Postal Code Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Postal Code Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Email Field Enabled	If enabled, displays a field for the user's e-mail on the form.
Email Field Required	If enabled, the user is required to complete this field on the form.
Email Field Label	Text label for the e-mail field on the form.
Email Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Email Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Phone Field Enabled	If enabled, displays a telephone number field on the form.
Phone Field Required	If enabled, the user is required to complete this field on the form.
Phone Field Label	Text label for the telephone number field on the form.
Phone Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Phone Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Hardware Description Field Enabled	If enabled, displays a field for to describe the user's hardware on the form.
Hardware Description Field Required	If enabled, the user is required to complete this field on the form.
Hardware Description Field Label	Text label for the hardware description field on the form.

Setting	Definition
Hardware Description Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Hardware Description Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Serial Number Field Enabled	If enabled, displays a field for the serial number of the user's PC or other device on the form.
Serial Number Field Required	If enabled, the user is required to complete this field on the form.
Serial Number Field Label	Text label for the field containing the serial number of the user's PC or other device on the form.
Serial Number Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Serial Number Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Hostname Field Enabled	If enabled, displays a field for the name of the user's PC or hostname on the form.
Hostname Field Required	If enabled, the user is required to complete this field on the form.
Hostname Field Label	Text label for the field containing the name of the user's PC or hostname on the form.
Hostname Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Hostname Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.

Standard User Registration Approval

Setting	Definition
Registrations Require Approval	Can be configured to either: • An Administrator with Self Registration Request Permissions • Any Administrator that belongs to a specified User group Administrators that belong to the group will be able to approve, regardless of their permissions. Administrators that do not belong to that group will be unable to approve. See the Admin Approval section for details.

Self registration login

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Left Column Content	Text displayed in the left column of the page.
Request Page Title	Text title for the first paragraph in the guest self registration request page.
Request Page Introduction	Text introduction on the guest self registration request page.
Request Page Form Title	Title of the self registration request guest form.
Request Access Button Text	Text displayed in the button to request guest access from the guest self registration page.
Pending Page Title	Text title for the first paragraph in the guest self registration request page.
Default Sponsor Email	Email of the sponsor(s) to send requests and/or notifications to. If this is not provided, the user will be required to enter this in. To enter multiple sponsors, the format is colon separated entries with each entry containing an email address and an optional display name separated by a comma. (eg. moe@example.com, Moe:curly@example.com.) This is a text-only field. No HTML or special characters, such as newlines, may be used. Attempting to include such content may produce unexpected results. (Versions 8.6.4, 8.7.2 and above) This field must be left blank if Required Sponsor Approval = None.
Sponsor Email Label	Label for the field to enter in the Sponsor's Email. This field only appears when there is no Default Sponsor Email.
Notify Sponsor of Guest Details	When enabled, sponsors will be notified of the Guests credentials through email and/or SMS.
Accept Notification	Text to notify the user that their guest request has been accepted.
Login Username Label	Label for the field to enter in the user name on the Guest Self Registration login page.
Login Password Label	Label for the field to enter in the password on the Guest Self Registration login page.

Setting	Definition
Require Sponsor Approval	When enabled, approval by a sponsor will be required before guest accounts will be created. Registration requests can be accessed under Users & Hosts > Registration Requests. Options: • None (Versions 8.6.4, 8.7.2 and above) If Required Sponsor Approval = None, the following steps are required: a. Set Default Sponsor Email = <blank> b. Set Required Sponsor Approval to something other than None. c. De-select Sponsor Approval Link Requires Login. d. Set Required Sponsor Approval back to None. • Email Addresses from an Allowed Domain: Any email address whose domain is listed in the "Allowed Sponsor Email Address Domains" field. User account does not have to exist in the FortiNAC database, but must be a valid account in the Domain. • Allowed Sponsor Email Address Domains: Option available when "Email Addresses from an Allowed Domain" is selected. A comma-separated list of domains that are allowed to receive Self Registration requests. Domain must be searchable by FortiNAC. • Any User • Any User in Group • Any Administrator • An Administrator with Self Registration Permissions
Guest Request Expiration (minutes)	Number of minutes that guest request will remain valid. After this time, a sponsor will no longer be able to approve this request.
Request Pending Message	Text to display in the Self Registration Request pending page.
Deny Notification	Text to notify the user that their guest request has been denied.
Expired Notification	Text to notify the user that their guest request has expired.
Cancel Request Button Text	Text displayed in the button to cancel a guest request.
Message from Sponsor Header	Header for the Message from the Sponsor.
Sponsor Email Intro Text	When sponsor approval is required, this text will appear before the html link in the email that is sent to the sponsor.
Sponsor Approval Link Requires Login	When enabled, the html link the sponsor receives in email will require them to login before approving or denying the request. If disabled, clicking on an approve or deny link will approve or deny the request without further interaction. This field will not display if Required Sponsor Approval = None. In order to modify, change this field to something else, then modify.
Use Secure Mode for Sponsor Approval Links	When enabled, secure html links will be used to approve or deny requests in the email the sponsor receives.

Setting	Definition
Sponsor Email Login Link Text	Text for the login link in the email sent to the sponsor. Only used when Sponsor Approval Link Requires Login is selected.
Sponsor Email Approve Link Text	Text for the approve link in the email sent to the sponsor. Only used when Sponsor Approval Link Requires Login is not selected.
Sponsor Email Deny Link Text	Text for the deny link in the email sent to the sponsor. Only used when Sponsor Approval Link Requires Login is not selected.
Notify User via Portal Page	When enabled, guest user will be notified of their credentials in the portal page.
Show Password in Portal Page Notification	When enabled and Notify User via Portal Page is enabled, the guest account password will be displayed in plain text in the login form.
Notify User via Email	When enabled, guest user will be notified of their credentials through email.
Notify User via SMS	When enabled, guest user will be notified of their credentials through a SMS Message.
Default Guest Template	Name of the Default Guest Template to use.
Acceptable Use Policy	Options for displaying or not displaying an Acceptable Use Policy.
Acceptable Use Policy Checkbox Text	Text label for the checkbox to agree to the Acceptable Use Policy.
URL for Acceptable Use Policy	Optional URL to an Acceptable Use Policy which the user must agree to before being allowed to log in.
Link text for Acceptable Use Policy URL	Optional URL to an Acceptable Use Policy which the user must agree to before being allowed to log in.
Text for Acceptable Use Policy	Optional Text for an Acceptable Use Policy which the user must agree to before being allowed to log in.
Instructions	Select whether instructions will be included in this page, as a link to Instructions, or not at all. Instruction are entered in the Content Editor under Registration-Instructions.
Sponsor Input Type	The form element to display for users to select or input their sponsor. Available options: • Hidden: User is not presented with a "Sponsor Email" field. Hidden should only be used with a default sponsor. • Input: "Sponsor Email" field is displayed. User must enter the sponsor's email. Email is validated based upon "Require Sponsor Approval" configuration. • Select: "Sponsor Email" field is displayed with drop down menu. Drop down menu is populated based upon entries in the "Default Sponsor Email" field. If "Default Sponsor Email" field is blank, no entries are presented in the "Sponsor Email" menu. • LDAP Group: Requires configuration of the "Sponsor LDAP Group" and "Sponsor Option Template" fields. The "Sponsor Email" field is displayed.

Setting	Definition
	User must enter the sponsor's email. If email is found within one of the LDAP groups specified under "Sponsor LDAP Group," the email will autocomplete. If the email is not found and user clicks the "Request Access" button, they will be presented with the message "Sponsor does not exist". User is then returned to the Self-Registration page.
Sponsor LDAP Group	An LDAP lookup searches for matching sponsors as the Sponsor field is filled out in the Guest Self Registration page of the FortiNAC captive portal. This function can be used to auto-fill the entry and displays matching searches' full name and email address. What is displayed is configurable so that the email address is not shown. In order to locate the user, NAC searches the group name specified in the Sponsor LDAP Group field. The group is matched against the "memberOf" attribute on the record in LDAP. The list of values for memberOf must contain the group as part of the query. Required Format: CN=<group name>,OU=<organizational unit>,DC=<2nd level domain name>,DC=<1st level domain name> To identify group branches searched by FortiNAC, navigate to System > Settings > Authentication > LDAP Click on the desired directory and click Modify Click Search Branches To view the group names imported from the directory, click Select groups Example: CN=Employees,OU=MainBldg,DC=example,DC=com 1. User types "Hof" in the portal 2. NAC searches to see if Hof* is a memberOf CN=<Employees> 3. Portal Returns a drop down of possible sponsors matching the first three character "Hof" for First name, Last name or Email
Sponsor Message Template	The template used when generating an email to the Sponsor of the guest account registration request. This template is provided various properties from the portal configuration to allow the Administrator to write a single template that covers all use cases. In addition to details regarding the request itself, the following fields are provided to the template: Sponsor Email Intro Text Sponsor Approval Link Requires Login Sponsor Email Login Link Text Sponsor Email Approve Link Text Sponsor Email Deny Link Text
Guest Details Message Template	A message sent to the guest at their provided email address following the approval of their account creation. Depending on the selection within the Guest Template, this email may also include their generated password. This is typically used to provide guests information regarding details of their account, such as the start and end date.

Setting	Definition
Guest Password Message Template	For customers with a security policy that requires the passwords be sent separately, this message is only provided the generated password. It will be sent immediately after the Guest Details message.
Message Template	The SMS message template containing the Guest details. Due to limitations of SMS, this is provided as a separate template so an Administrator may supply a simplified message following the approval of a guest account. This message type is the same as the Guest Details Message Template.

Guest Login

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the first paragraph in the primary guest login page. Displays above the text entered in the Introduction property.
Left Column Content	Text displayed in the left column of the page.
Introduction	Text introduction to the primary login for Guests and Contractors.
Form Title	Title of the guest registration form.
Username Label	Label for the user name field.
Password Label	Label for the password field.
Missing Fields	Message displayed when required fields are missing.
Instructions	Select whether instructions will be included in this page, as a link to Instructions, or not at all. Instruction are entered in the Content Editor under Registration-Instructions.

Secondary guest login

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the first paragraph in the secondary guest login page. Displays above the text entered in the Introduction property.
Left Column Content	Text displayed in the left column of the page.
Main Content	Text content displayed above the login form.
Introductory Paragraph	Introduction text displayed above the Main Content property in the page.
Form Button Text	Text displayed in the form button.
Account Expiration Label	Label for displaying the account expiration information.
Login Availability Label	Label for displaying the assailable times to log in.

Guest User Registration Approval

Setting	Definition
Registrations Require Approval	Can be configured to either: • An Administrator with Self Registration Request Permissions • Any Administrator that belongs to a specified User group Administrators that belong to the group will be able to approve, regardless of their permissions. Administrators that do not belong to that group will be unable to approve. See the Admin Approval section for details.

Anonymous authentication

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Left Column Content	Text displayed in the left column of the page.
Role	The role to apply to guests who authenticate anonymously.
Acceptable Use Policy	Options for displaying or not displaying an Acceptable Use Policy.
Acceptable Use Policy Checkbox Text	Text label for the checkbox to agree to the Acceptable Use Policy.
URL for Acceptable Use Policy	Optional URL to an Acceptable Use Policy which the user must agree to before being allowed to log in.
Link text for Acceptable Use Policy URL	Optional URL to an Acceptable Use Policy which the user must agree to before being allowed to log in.
Text for Acceptable Use Policy	Optional Text for an Acceptable Use Policy which the user must agree to before being allowed to log in.

Game device registration

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Form Title	Title of the game console registration form.
Left Column Content	Text displayed in the left column of the page.
Introduction	Text introducing the purpose of the game console registration page.
Description	Text describing the registration process for game consoles.

Setting	Definition
IP address Field Enabled	If enabled, shows a field where the user may enter the IP address of their gaming device.
IP address Label	Label of the IP address form field.
Device Type Field Enabled	If enabled, shows a select box to select the device type as defined in the Device Types field.
Device Type Label	The text label for the Device Type form field.
Device Types (Value,Name : Value, Name)	Example: "Wii,Nintendo Wii : XBox 360 : Microsoft XBox 360
Device Type Error	The error displayed when a device type has not been selected.
MAC Address Example	Example MAC Address
IP address Example	Example IP address.
Role Field Enabled	If enabled, network access is limited based on the Role Name in the Role Field Value field and the roles created under Go - Manage - Roles. Roles provide location-based access control.
Role Field Label	Text label for the Role field on the form.
Role Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Role Field Value	Data entry field used to submit data with the form. Requires a role name. Roles are used to control network access. Typically this field is set by the administrator with the field type set to hidden. Role names must match those in the database. You can also create a list of roles for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green.
Validate Gaming Device OUI	When enabled, a valid gaming device OUI is required for registration using the Game Device Registration portal. When not enabled, a gaming device OUI is not required, meaning that any host can be registered using the Game Device Registration portal. This allows a host without access to a web browser, such as a printer, to be registered through the Game Device Registration portal.
Invalid MAC Address Error	Error message displayed to the user when the MAC address entered was invalid.
Invalid IP address Error	Error message displayed to the user when the IP address entered was invalid.

Game device help

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.

Setting	Definition
Title	Text title for the help page for gaming devices. Displays above the text entered in the Content property.
Left Column Content	Text displayed in the left column of the page.
Content	Instructional text on how to find the MAC addresses of specific game consoles.

Custom login

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the first paragraph in the custom login page. Displays above the text entered in the Introduction property.
Left Column Content	Text displayed in the left column of the page.
Introduction	Text introduction for the custom login page.
Secondary Text	Additional text which displays below the text entered in the Introduction property.
Instructions	Select whether instructions will be included in this page, as a link to Instructions, or not at all. Instruction are entered in the Content Editor under Registration-Instructions.

Custom login form

Setting	Definition
Form Title	Title of the form field set.
Form Action	Redirects the user to the next page in the sequence.
	 Changing the form action to an unsupported page may affect functionality.
Success Page (Relative)	Relative URL to the success message.
	 Changing this may affect supported functionality.
Missing Fields Message	Message displayed to the user if all required fields on the form are not completed.

Setting	Definition
Host Expiration Period Enabled	If enabled, the amount of time that the host can access the network is limited to the time entered in the Host Expiration Period Value field. The Host Expiration Period Value field defaults to hidden. The time value provided by the Administrator and is submitted with the rest of the form data.
Host Expiration Period Unit	The Unit of measurement for the amount of time that the host will be registered before expiry
Host Expiration Period Value	The amount of time that the host will be registered before expiry
Username Field Enabled	If enabled, displays a Username field on the form.
Username Field Required	If enabled, the user is required to complete this field on the form.
Username Field Label	Text label for the Username field on the form.
Username Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Username Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Password Field Enabled	If enabled, displays a password field on the form.
Password Field Required	If enabled, the user is required to complete this field on the form.
Password Field Label	Text label for password field on the form.
Password Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Password Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
First Name Field Enabled	If enabled, displays a First Name field on the form.
First Name Field Required	If enabled, the user is required to complete this field on the form.
First Name Field Label	Text label for the First Name field on the form.
First Name Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.

Setting	Definition
First Name Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Last Name Field Enabled	If enabled, displays a Last Name field on the form.
Last Name Field Required	If enabled, the user is required to complete this field on the form.
Last Name Field Label	Text label for the Last Name field on the form.
Last Name Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Last Name Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Security and Access Value (S&A) Field Enabled	If enabled, displays a field for the Security and Access Value on the form.
S&A Field Required	If enabled, the user is required to complete the Address field on the form.
S&A Field Label	Text label for the S&A field on the form.
S&A Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
S&A Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Role Field Enabled	If enabled, network access is limited based on the Role Name in the Role Field Value field and the roles created under Go - Manage - Roles. Roles provide location-based access control.
Role Field Required	If enabled, the user is required to complete this field on the form.
Role Field Label	Text label for the Role field on the form.
Role Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.

Setting	Definition
Role Field Value	Data entry field used to submit data with the form. Requires a role name. Roles are used to control network access. Typically this field is set by the administrator with the field type set to hidden. Role names must match those in the database. You can also create a list of roles for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green.
Title Field Enabled	If enabled, displays a field for the user's title on the form.
Title Field Required	If enabled, the user is required to complete this field on the form.
Title Field Label	Text label for the title field on the form.
Title Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Title Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Address Field Enabled	If enabled, displays a field for the user's address on the form.
Address Field Required	If enabled, the user is required to complete the Address field on the form.
Address Field Label	Text label for the Address field on the form.
Address Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Address Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
City Field Enabled	If enabled, displays a field for the user's city on the form.
City Field Required	If enabled, the user is required to complete this field on the form.
City Field Label	Text label for the City field on the form.
City Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.

Setting	Definition
City Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
State/Province Field Enabled	If enabled, displays a State/Province field on the form.
State/Province Field Required	If enabled, the user is required to complete this field on the form.
State/Province Field Label	Text label for the State/Province field on the form.
State/Province Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
State/Province Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Postal Code Field Enabled	If enabled, displays a Postal Code field on the form.
Postal Code Field Required	If enabled, the user is required to complete this field on the form.
Postal Code Field Label	Text label for the Postal Code field on the form.
Postal Code Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Postal Code Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Email Field Enabled	If enabled, displays a field for the user's e-mail on the form.
Email Field Required	If enabled, the user is required to complete this field on the form.
Email Field Label	Text label for the e-mail field on the form.
Email Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.

Setting	Definition
Email Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Phone Field Enabled	If enabled, displays a telephone number field on the form.
Phone Field Required	If enabled, the user is required to complete this field on the form.
Phone Field Label	Text label for the telephone number field on the form.
Phone Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Phone Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Hardware Description Field Enabled	If enabled, displays a field for to describe the user's hardware on the form.
Hardware Description Field Required	If enabled, the user is required to complete this field on the form.
Hardware Description Field Label	Text label for the hardware description field on the form.
Hardware Description Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Hardware Description Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Serial Number Field Enabled	If enabled, displays a field for the serial number of the user's PC or other device on the form.
Serial Number Field Required	If enabled, the user is required to complete this field on the form.
Serial Number Field Label	Text label for the field containing the serial number of the user's PC or other device on the form.

Setting	Definition
Serial Number Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Serial Number Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Hostname Field Enabled	If enabled, displays a field for the host name of the user's PC or other device on the form.
Hostname Field Required	If enabled, the user is required to complete this field on the form.
Hostname Field Label	Text label for the field containing the name of the user's PC or hostname on the form.
Hostname Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Hostname Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.

Custom User Registration Approval

Setting	Definition
Registrations Require Approval	Can be configured to either: • An Administrator with Self Registration Request Permissions • Any Administrator that belongs to a specified User group Administrators that belong to the group will be able to approve, regardless of their permissions. Administrators that do not belong to that group will be unable to approve. See the Admin Approval section for details.

MDM registration

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.

Setting	Definition
Title	Text title for the first paragraph in the login page. Displays above the text entered in the Introduction property.
Left Column Content	Text displayed in the left column of the page.
Header	Text displayed above the links to the MDM apps.
Content	The main body text for the MDM Providers. This text should include all links to the MDM apps for each operating system.

Profile configuration download

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Left Column Content	Text displayed in the left column of the page.
Introduction	Introductory text explaining what steps need to be taken.
Download Link Prefix	Text displayed before the download link.
Download Link	Text displayed as a link.
Download Link Suffix	Text displayed after the download link.
Button Text	Text displayed on the button on the profile download page.

Mobile Agent download

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Left Column Content	Text displayed in the left column of the page.
Profile Introduction	Introductory text explaining what steps need to be taken with respect to configuration profile installation.
Profile Download Link Prefix	Text displayed before the profile download link.
Profile Download Link	Text displayed as a link.
Profile Download Link Suffix	Text displayed after the profile download link.
Introduction	Introductory text explaining what steps need to be taken.
Download Link Prefix	Text displayed before the download link.
Download Link	Text displayed as a link.
Download Link Suffix	Text displayed after the download link.

Instructions

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the instructions page. Displays above the text entered in the Introduction property.
Left Column Content	Text displayed in the left column of the page.
Introduction	Text introduction to the instructions page.
Show Windows Instructions	If enabled, display instructions for computers running Windows.
Windows Instructions	Instructional text for computers running Windows.
Show macOS Instructions	If enabled, display instructions for computers running macOS.
macOS Instructions	Instructional text for computers running macOS.
Show Linux Instructions	If enabled, display instructions for computers running Linux.
Linux Instructions	Instructional text for computers running Linux.
Show Other Instructions	If enabled, display instructions for other computers.
Other Instructions Title	Text displayed as the title for the instructions for other computers.
Other Instructions	Instructional text for other computers.
Display as Accordion View	Use JavaScript to display the instructions as an accordion. Requires the global "Use JavaScript UI Enhancements" property to be enabled.

Acceptable Use Policy

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the usage policy. Displays above the text entered in the Usage Policy Contents property.
Left Column Content	Text displayed in the left column of the page.
Usage Policy Contents	Contents of the Usage Policy.

Usage policy disagreement

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.

Setting	Definition
Title	Text title for the first paragraph in Acceptable Use Policy Disagreement page. Displays above the text entered in the Disagree Instructions property.
Left Column Content	Text displayed in the left column of the page.
Disagree Instructions	Instructional text for users who disagree with the usage policy.
Start Again Instructions	Instructions for getting back to the usage policy.

Client certificate download

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the Client Certificate Download page. Displays above the text entered in the Introduction property.
Left Column Content	Text displayed in the left column of the page.
Introduction	Text introduction to the instructions page.
Secondary Text	Text displayed in the second paragraph of the certificate download page. This is an HTML field and HTML may be freely entered in this field.
Session Expired Message	Text displayed when the server is unable to find an existing session to determine the user who is currently logged into the portal. This field contains contents which are output as strings in JavaScript. Certain special characters may be escaped or removed.
Missing Certificate Message	Text displayed when no existing certificate could be found for the user. This is a mixed text field. HTML may be included, but may not always be rendered.
Download Link Prefix	Text displayed before the download link. This is a mixed text field. HTML may be included, but may not always be rendered.
Download Link	Text displayed as a link. This is a mixed text field. HTML may be included, but may not always be rendered.
Download Link Suffix	Text displayed after the download link. This is a mixed text field. HTML may be included, but may not always be rendered.
Resubmit Request Link Prefix	Text displayed before the download link. This is a mixed text field. HTML may be included, but may not always be rendered.
Resubmit Request Link	Text displayed as a link. This is a mixed text field. HTML may be included, but may not always be rendered.
Resubmit Request Link Suffix	Text displayed after the download link. This is a mixed text field. HTML may be included, but may not always be rendered.
Continue Link Prefix	Text displayed before the download link. This is a mixed text field. HTML may be included, but may not always be rendered.

Setting	Definition
Continue Link	Text displayed as a link. This is a mixed text field. HTML may be included, but may not always be rendered.
Continue Link Suffix	Text displayed after the download link. This is a mixed text field. HTML may be included, but may not always be rendered.

Success

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the success page. Indicates that the user has successfully registered. Displays at the top of the content section.
Left Column Content	Text displayed in the left column of the page.
Progress Bar Enabled	If checked, display a progress bar and display the Finished Message.
Progress Bar Title	Title displayed above all text in the contents pane.
Please Wait Message	Message displayed to the user while the progress bar moves. To change the amount of time the message and progress bar are displayed, modify the default 45 second countdown number.
Success Message	Message displayed to indicate successful completion of the process.
Finished Message	Appears after the progress bar has finished.

Admin Approval (Version 8.8.2 and above)

Applies to the following Captive Portal Login Processes

- Standard User
- Guest
- Custom

Note: This feature does not affect registration through any other process, such as Persistent Agent or WMI.

When registering through the portal and immediately following authentication of the user's credentials, the device is placed in a "Pending Approval" state. Upon Administrator approval, the portal notifies the user and allows them to complete the Registration process for the device.

This feature is configured individually per login process. A host registration request may be configured to either be approved by:

- An Administrator with Self Registration Request permissions
- Any Administrator that belongs to a specified User group.

Administrators that belong to the group will be able to approve, regardless of their permissions. Administrators that do not belong to that group will be unable to approve.

Configure Registration Approval using the appropriate branches of the Registration section of the Content Editor:

- Standard User Registration Approval
- Guest Registration Approval
- Customer Registration Approval

Authentication

Configure the settings and behavior of your portal pages for authenticating hosts on your network. This includes settings for remote scanning.

Common

Setting	Definition
Context Title	Text label to indicate the functional purpose of the context.

Login menu

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the first paragraph in the guest login page. Displays above the text entered in the Introduction property.
Left Column Content	Text displayed in the left column of the login page.
Text Content	Text introducing the login menu for Authentication.
Standard Login Enabled	When enabled, the Standard login option appears in the login menu.
Standard Login Title	Short text to indicate who should use the standard login.
Standard Login Link	Text displayed below the link for the Standard login.
Standard Login Order	Integer value indicating the order this item should appear in on the page.
Guest Login Enabled	When enabled, the Guest Login option appears in the login menu.
Guest Login Title	Short text to indicate who should use the standard login.
Guest Login Link	Text displayed as a link to the Guest Access page.
Guest Login Order	Integer value indicating the order this item should appear in on the page.
Custom Registration Enabled	If enabled, the Custom Registration Option appears in the login menu.
Custom Registration Title	Text label above the link to the custom registration.
Custom Registration Link Text	Text displayed in the link for a custom device registration, such as a mobile device.
Custom Registration Order	Integer value indicating the order this item should appear in on the page.

Standard user login

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Title displayed above the contents of the Introduction property.
Left Column Content	Text displayed in the left column of the login page.
Introduction	Text introduction to the Standard Login page.
Secondary Text	Text displayed above the login form.
Instructions	Select whether instructions will be included in this page, as a link to Instructions, or not at all. Instruction are entered in the Content Editor under Authentication-Instructions.
Scan Registered Hosts	If enabled, scan the host using Dissolvable or Persistent Agent, if a Security Policy is applicable.
Scan Rogue Hosts	If enabled, scan a rogue host using Dissolvable or Persistent Agent, if a Security Policy is applicable.
Register Rogue Hosts	If enabled, register a rogue host.

Standard user login form

Setting	Definition
Form Title	Text title of the login form field set.
Form Action	Redirects the user to the next page in the sequence.  Changing the form action to an unsupported page may affect functionality.
Success Page (Relative)	Relative URL to the success message.  Changing this may affect supported functionality.
Missing Fields Message	Message displayed to the user if all required fields on the form are not completed.

Setting	Definition
Host Expiration Period Enabled	If enabled, the amount of time that the host can access the network is limited to the time entered in the Host Expiration Period Value field. The Host Expiration Period Value field defaults to hidden. The time value provided by the Administrator and is submitted with the rest of the form data.
Host Expiration Period Unit	The Unit of measurement for the amount of time that the host will be registered before expiry.
Host Expiration Period Value	The amount of time that the host will be registered before expiry.
Username Field Enabled	If enabled, displays a Username field on the form.
Username Field Required	If enabled, the user is required to complete this field on the form.
Username Field Label	Text label for the Username field on the form.
Username Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Username Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Password Field Enabled	If enabled, displays a password field on the form.
Password Field Required	If enabled, the user is required to complete this field on the form.
Password Field Label	Text label for password field on the form.
Password Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Password Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
First Name Field Enabled	If enabled, displays a First Name field on the form.
First Name Field Required	If enabled, the user is required to complete this field on the form.
First Name Field Label	Text label for the First Name field on the form.
First Name Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.

Setting	Definition
First Name Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Last Name Field Enabled	If enabled, displays a Last Name field on the form.
Last Name Field Required	If enabled, the user is required to complete this field on the form.
Last Name Field Label	Text label for the Last Name field on the form.
Last Name Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Last Name Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Security and Access Value (S&A) Field Enabled	If enabled, displays a field for the Security and Access Value on the form.
S&A Field Required	If enabled, the user is required to complete the Address field on the form.
S&A Field Label	Text label for the S&A field on the form.
S&A Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
S&A Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Role Field Enabled	If enabled, network access is limited based on the Role Name in the Role Field Value field and the roles created under Go - Manage - Roles. Roles provide location-based access control.
Role Field Required	If enabled, the user is required to complete this field on the form.
Role Field Label	Text label for the Role field on the form.
Role Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.

Setting	Definition
Role Field Value	Data entry field used to submit data with the form. Requires a role name. Roles are used to control network access. Typically this field is set by the administrator with the field type set to hidden. Role names must match those in the database. You can also create a list of roles for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green.
Title Field Enabled	If enabled, displays a field for the user's title on the form.
Title Field Required	If enabled, the user is required to complete this field on the form.
Title Field Label	Text label for the title field on the form.
Title Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Title Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Address Field Enabled	If enabled, displays a field for the user's address on the form.
Address Field Required	If enabled, the user is required to complete the Address field on the form.
Address Field Label	Text label for the Address field on the form.
Address Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Address Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
City Field Enabled	If enabled, displays a field for the user's city on the form.
City Field Required	If enabled, the user is required to complete this field on the form.
City Field Label	Text label for the City field on the form.
City Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.

Setting	Definition
City Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
State/Province Field Enabled	If enabled, displays a State/Province field on the form.
State/Province Field Required	If enabled, the user is required to complete this field on the form.
State/Province Field Label	Text label for the State/Province field on the form.
State/Province Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
State/Province Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Postal Code Field Enabled	If enabled, displays a Postal Code field on the form.
Postal Code Field Required	If enabled, the user is required to complete this field on the form.
Postal Code Field Label	Text label for the Postal Code field on the form.
Postal Code Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Postal Code Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Email Field Enabled	If enabled, displays a field for the user's e-mail on the form.
Email Field Required	If enabled, the user is required to complete this field on the form.
Email Field Label	Text label for the e-mail field on the form.
Email Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.

Setting	Definition
Email Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Phone Field Enabled	If enabled, displays a telephone number field on the form.
Phone Field Required	If enabled, the user is required to complete this field on the form.
Phone Field Label	Text label for the telephone number field on the form.
Phone Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Phone Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Organization Field Enabled	If enabled, displays a organization field on the form.
Organization Field Required	If enabled, the user is required to complete this field on the form.
Organization Field Label	Text label for the organization field on the form.
Organization Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Organization Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Hardware Description Field Enabled	If enabled, displays a field for to describe the user's hardware on the form.
Hardware Description Field Required	If enabled, the user is required to complete this field on the form.
Hardware Description Field Label	Text label for the hardware description field on the form.
Hardware Description Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.

Setting	Definition
Hardware Description Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Serial Number Field Enabled	If enabled, displays a field for the serial number of the user's PC or other device on the form.
Serial Number Field Required	If enabled, the user is required to complete this field on the form.
Serial Number Field Label	Text label for the field containing the serial number of the user's PC or other device on the form.
Serial Number Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Serial Number Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Hostname Field Enabled	If enabled, displays a field for the name of the user's PC or hostname on the form.
Hostname Field Required	If enabled, the user is required to complete this field on the form.
Hostname Field Label	Text label for the field containing the name of the user's PC or hostname on the form.
Hostname Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Hostname Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.

Primary guest login

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for guest login and authentication page. Displays at the top of the

Setting	Definition
	content section of the page above the Introduction property.
Left Column Content	Text displayed in the left column of the page.
Introduction	Introductory text to describe the Guest process.
Form Title	Title of the guest authentication form.
Username Label	Label for the user name field.
Password Label	Label for the password field.
Missing Fields	Message displayed when required fields are missing.
Instructions	Select whether instructions will be included in this page, as a link to Instructions, or not at all. Instruction are entered in the Content Editor under Authentication-Instructions.

Secondary guest login

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the first paragraph in the secondary guest login page. Displays above the text entered in the Introduction property.
Left Column Content	Text displayed in the left column of the page.
Main Content	Text content displayed above the login form.
Introductory Paragraph	Introduction text displayed above the Main Content property in the page.
Form Button Text	Text displayed in the form button.
Account Expiration Label	Label for displaying the account expiration information.
Login Availability Label	Label for displaying the available times to log in.

Custom login

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the first paragraph in the custom login page. Displays above the text entered in the Introduction property.
Left Column Content	Text displayed in the left column of the page.
Introduction	Text introduction for the custom login page.
Secondary Text	Additional text which displays below the text entered in the Introduction property.

Setting	Definition
Instructions	Select whether instructions will be included in this page, as a link to Instructions, or not at all. Instruction are entered in the Content Editor under Authentication-Instructions.
Scan Registered Hosts	If enabled, scan the host using Dissolvable or Persistent Agent, if a Security Policy is applicable.
Scan Rogue Hosts	If enabled, scan a rogue host using Dissolvable or Persistent Agent, if a Security Policy is applicable.
Register Rogue Hosts	If enabled, register a rogue host.

Custom login form

Setting	Definition
Form Title	Title of the form field set.
Form Action	Redirects the user to the next page in the sequence.  Changing the form action to an unsupported page may affect functionality.
Success Page (Relative)	Relative URL to the success message.  Changing this may affect supported functionality.
Missing Fields Message	Message displayed to the user if all required fields on the form are not completed.
Host Expiration Period Enabled	If enabled, the amount of time that the host can access the network is limited to the time entered in the Host Expiration Period Value field. The Host Expiration Period Value field defaults to hidden. The time value provided by the Administrator and is submitted with the rest of the form data.
Host Expiration Period Unit	The Unit of measurement for the amount of time that the host will be registered before expiry
Host Expiration Period Value	The amount of time that the host will be registered before expiry.
Username Field Enabled	If enabled, displays a Username field on the form.
Username Field Required	If enabled, the user is required to complete this field on the form.
Username Field Label	Text label for the Username field on the form.

Setting	Definition
Username Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Username Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Password Field Enabled	If enabled, displays a password field on the form.
Password Field Required	If enabled, the user is required to complete this field on the form.
Password Field Label	Text label for password field on the form.
Password Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Password Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
First Name Field Enabled	If enabled, displays a First Name field on the form.
First Name Field Required	If enabled, the user is required to complete this field on the form.
First Name Field Label	Text label for the First Name field on the form.
First Name Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
First Name Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Last Name Field Enabled	If enabled, displays a Last Name field on the form.
Last Name Field Required	If enabled, the user is required to complete this field on the form.
Last Name Field Label	Text label for the Last Name field on the form.

Setting	Definition
Last Name Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Last Name Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Security and Access Value (S&A) Field Enabled	If enabled, displays a field for the Security and Access Value on the form.
S&A Field Required	If enabled, the user is required to complete the Address field on the form.
S&A Field Label	Text label for the S&A field on the form.
S&A Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
S&A Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Role Field Enabled	If enabled, network access is limited based on the Role Name in the Role Field Value field and the roles created under Go - Manage - Roles. Roles provide location-based access control.
Role Field Required	If enabled, the user is required to complete this field on the form.
Role Field Label	Text label for the Role field on the form.
Role Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Role Field Value	Data entry field used to submit data with the form. Requires a role name. Roles are used to control network access. Typically this field is set by the administrator with the field type set to hidden. Role names must match those in the database. You can also create a list of roles for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green.
Title Field Enabled	If enabled, displays a field for the user's title on the form.
Title Field Required	If enabled, the user is required to complete this field on the form.
Title Field Label	Text label for the title field on the form.

Setting	Definition
Title Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Title Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Address Field Enabled	If enabled, displays a field for the user's address on the form.
Address Field Required	If enabled, the user is required to complete the Address field on the form.
Address Field Label	Text label for the Address field on the form.
Address Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Address Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
City Field Enabled	If enabled, displays a field for the user's city on the form.
City Field Required	If enabled, the user is required to complete this field on the form.
City Field Label	Text label for the City field on the form.
City Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
City Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
State/Province Field Enabled	If enabled, displays a State/Province field on the form.
State/Province Field Required	If enabled, the user is required to complete this field on the form.
State/Province Field Label	Text label for the State/Province field on the form.

Setting	Definition
State/Province Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
State/Province Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Postal Code Field Enabled	If enabled, displays a Postal Code field on the form.
Postal Code Field Required	If enabled, the user is required to complete this field on the form.
Postal Code Field Label	Text label for the Postal Code field on the form.
Postal Code Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Postal Code Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Email Field Enabled	If enabled, displays a field for the user's e-mail on the form.
Email Field Required	If enabled, the user is required to complete this field on the form.
Email Field Label	Text label for the e-mail field on the form.
Email Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Email Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Phone Field Enabled	If enabled, displays a telephone number field on the form.
Phone Field Required	If enabled, the user is required to complete this field on the form.
Phone Field Label	Text label for the telephone number field on the form.

Setting	Definition
Phone Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Phone Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Organization Field Enabled	If enabled, displays a organization field on the form.
Organization Field Required	If enabled, the user is required to complete this field on the form.
Organization Field Label	Text label for the organization field on the form.
Organization Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Organization Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Hardware Description Field Enabled	If enabled, displays a field for to describe the user's hardware on the form.
Hardware Description Field Required	If enabled, the user is required to complete this field on the form.
Hardware Description Field Label	Text label for the hardware description field on the form.
Hardware Description Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Hardware Description Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Serial Number Field Enabled	If enabled, displays a field for the serial number of the user's PC or other device on the form.
Serial Number Field Required	If enabled, the user is required to complete this field on the form.

Setting	Definition
Serial Number Field Label	Text label for the field containing the serial number of the user's PC or other device on the form.
Serial Number Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Serial Number Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Hostname Field Enabled	If enabled, displays a field for the host name of the user's PC or other device on the form.
Hostname Field Required	If enabled, the user is required to complete this field on the form.
Hostname Field Label	Text label for the field containing the name of the user's PC or hostname on the form.
Hostname Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Hostname Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.

Remote scan index

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for remote scan index page. Displays at the top of the content section of the page.
Left Column Content	Text displayed in the left column of the page.
Scan Name	Name of the security policy to scan remote computers against.
Description	Brief description and instructional text for the Remote Scan process.

Remote scan success

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for remote scan success page. Displays at the top of the content section of the page.
Left Column Content	Text displayed in the left column of the page.
Success Message	Message displayed to the user after the remote scanning process completed successfully.

Log off form

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the log off form. Displays above the logout fields.
Left Column Content	Text displayed in the left column of the page.
Description	Text displayed above the Logout button.

Log off success

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title displayed above the Success Message.
Left Column Content	Text displayed in the left column of the page.
Success Message	Message displayed upon successful log off.

Authentication failure

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for authentication failure page. Displays at the top of the content section of the page.
Left Column Content	Text displayed in the left column of the page.
Description	Failure Text displayed when the user failed to authenticate.

Mobile Agent download

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Left Column Content	Text displayed in the left column of the page.
Introduction	Introductory text explaining what steps need to be taken.
Download Link Prefix	Text displayed before the download link.
Download Link	Text displayed as a link.
Download Link Suffix	Text displayed after the download link.

Profile configuration download

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Left Column Content	Text displayed in the left column of the page.
Introduction	Introductory text explaining what steps need to be taken.
Download Link Prefix	Text displayed before the download link.
Download Link	Text displayed as a link.
Download Link Suffix	Text displayed after the download link.
Button Text	Text displayed on the button on the profile download page.

Instructions

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the instructions page. Displays at the top of the content section of the page above the Introduction property.
Left Column Content	Text displayed in the left column of the page.
Introduction	Introductory text explaining what steps need to be taken.
Show Windows Instructions	If enabled, displays instructions for computers running Windows.
Windows Instructions	Instructions for computers running Windows.
Show macOS Instructions	If enabled, displays instructions for computers running macOS.
macOS Instructions	Instructions for computers running macOS.

Setting	Definition
Show Linux Instructions	If enabled, shows instructions for computers running Linux.
Linux Instructions	Instructions for computers running Linux.
Show Other Instructions	If enabled, show instructions for other computers.
Other Instructions Title	Text title of the instructions for other computers.
Other Instructions	Instructions for other computers.
Display as Accordion View	Use JavaScript to display the instructions as an accordion.

Success

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title displayed above the Success Message contents.
Left Column Content	Text displayed in the left column of the page.
Progress Bar Enabled	If checked, display a progress bar and display the finished message.
Progress Bar Title	Text title for the progress bar.
Please Wait Message	Message displayed to the user while the progress bar moves. To change the amount of time the message and progress bar are displayed, modify the default 45 second countdown number.
Success Message	Message displayed to the user upon successful authentication.
Finished Message	Appears after the progress bar has finished.

Remediation

Configure the settings and behavior of your portal pages for hosts in remediation.

Common

Setting	Definition
Context Title	Text label to indicate the functional purpose of the context.

Index (redirect)

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.

Setting	Definition
Title	Title displayed above the Description property contents.
Left Column Content	Text displayed in the left column of the login page.
Description	Text describing what is happening.

Dissolvable Agent rescan (login)

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Title displayed above the Description property contents.
Form Title	Text label displayed at the top of the login form.
Left Column Content	Text displayed in the left column of the login page.
Instructions	Instructional text displayed above the login form.
Username Field Label	Text label for the Username field on the form.
Password Field Label	Text label for the Password field on the form.
Authenticate Users	If enabled, authenticate users upon successful scanning.
Missing Fields Message	Message displayed to the user if all required fields on the form are not completed.

Dissolvable Agent rescan (no login)

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Title displayed above the Instructions property contents.
Left Column Content	Text displayed in the left column of the login page.
Instructions	Instructional text displayed above the download form.

Agent download

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Left Column Content	Text displayed in the left column of the login page.
Introduction	Introductory text explaining what steps need to be taken.

Setting	Definition
Download Link Prefix	Text displayed before the download link.
Download Link	Text displayed as a link.
Download Link Suffix	Text displayed after the download link.

Profile configuration download

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Left Column Content	Text displayed in the left column of the login page.
Introduction	Introductory text explaining what steps need to be taken.
Download Link Prefix	Text displayed before the download link.
Download Link	Text displayed as a link.
Download Link Suffix	Text displayed after the download link.
Button Text	Text displayed on the button on the profile download page.

Mobile Agent download

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Left Column Content	Text displayed in the left column of the login page.
Introduction	Introductory text explaining what steps need to be taken.
Download Link Prefix	Text displayed before the download link.
Download Link	Text displayed as a link.
Download Link Suffix	Text displayed after the download link.

Instructions

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Title displayed above the Introduction property contents.
Left Column Content	Text displayed in the left column of the login page.
Introduction	Introductory text explaining what steps need to be taken.

Setting	Definition
Show Windows Instructions	If enabled, display instructions for computers running Windows.
Windows Instructions	Instructional text for computers running Windows.
Show macOS Instructions	If enabled, display instructions for computers running macOS.
macOS Instructions	Instructional text for computers running macOS.
Show Linux Instructions	If enabled, display instructions for computers running Linux.
Linux Instructions	Instructional text for computers running Linux.
Show Other Instructions	If enabled, display instructions for other computers.
Other Instructions Title	Title of the instructions for other computers.
Other Instructions	Instructional text for other computers.
Display as Accordion View	Use JavaScript to display the instructions as an accordion.

Failure index

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Title displayed above the lists of failures.
Contents	Expanded text contents displayed below the title.
Left Column Content	Text displayed in the left column of the page.
Use Active Scan	If enabled, the only Endpoint Compliance Scan failure that can be shown is the one associated with the host's current endpoint Compliance Policy. If the host does not match any policies, any failed scan can be displayed.

Success

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Title displayed above the Remediation Successful property contents.
Left Column Content	Text displayed in the left column of the page.
Please Wait Message	Message displayed to the user while the progress bar moves. To change the amount of time the message and progress bar are displayed, modify the default 45 second countdown number.
Finished Message	Message displayed when the progress bar finishes.
Remediation Successful	Text displayed when the remediation process is completed successfully.

Setting	Definition
Proactive Scan Successful	Text displayed when the Proactive Scan is completed successfully.
Progress Bar Enabled	If checked, display a progress bar and display the finished message.
Progress Bar Title	Title for the progress bar.

Dead end

Configure the settings and behavior of your portal pages for hosts in dead end.

Common

Setting	Definition
Context Title	Text label to indicate the functional purpose of the context.

Index

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Title displayed above the content property contents.
Left Column Content	Text displayed in the left column of the page.
Content	Text content displayed to the user.
Show Disabling Security Alarm	Select to display information in the portal to the user about why the user is in dead end.
Security Alarm Title	Text label for the title of the column displaying the security alarm.
Security Alarm Description	Text displayed for the security alarm description.
Show Alarm Rule Text	Select to display alarm rule text.
Show All Event Types	Select to display all event types.
Alert Type Header	Text displayed for the alert type column header.
Show All Event Subtypes	Select to display all event subtypes.
Subtype Header	Text displayed for the event subtype column header.
Show All Event Severities	Select to display severities for all events.
Severity Header	Text displayed for the severity column header.
Show All Event Thread IDs	Select to display threat IDs for all events.
Threat ID Header	Text displayed for the threat ID column header.

Setting	Definition
Show All Event Descriptions	Select to display descriptions for all events.
Event Description Header	Text displayed for the event description column header.
Custom Columns (Header, Column:Header, Column)	Text displayed for custom column headers.

VPN

Configure the settings and behavior of your portal pages specifically for VPN access.

Common

Setting	Definition
Context Title	Text label to indicate the functional purpose of the context.

Index (redirect)

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Title displayed above the Description property contents.
Left Column Content	Text displayed in the left column of the login page.
Description	Text describing the redirect.
Redirect Timeout	Time in seconds before being redirected to Agent Download/Login. This is a positive number field. Only whole numbers greater than or equal to zero may be used

Download page

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title for the first paragraph in the download page. Displays above the text entered in the Introduction property.
Left Column Content	Text displayed in the left column of the login page.
Introduction	Text displayed in the first paragraph of the regular network user login page.
Secondary Text	Text displayed in the second paragraph of the regular network user login page.
Instructions	Select whether instructions will be included in this page, as a link to Instructions, or not at all. Instruction are entered in the content editor under VPN instructions.

Download page form

Setting	Definition
Form Title	Text label displayed at the top of the login form.
Form Action	Redirects the user to the next page in the sequence.  Changing the form action to an unsupported page may affect functionality.
Success Page (Relative)	Relative URL to the success message.  Changing this may affect supported functionality.
Missing Fields Message	Message displayed to the user if all required fields on the form are not completed.
Host Expiration Period Enabled	If enabled, the amount of time that the host can access the network is limited to the time entered in the Host Expiration Period Value field. The Host Expiration Period Value field defaults to hidden. The time value provided by the Administrator and is submitted with the rest of the form data.
Host Expiration Period Unit	The Unit of measurement for the amount of time that the host will be registered before expiry.
Host Expiration Period Value	The amount of time that the host will be registered before expiry.
Username Field Enabled	If enabled, displays a Username field on the form.
Username Field Required	If enabled, the user is required to complete this field on the form.
Username Field Label	Text label for the Username field on the form.
Username Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Username Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Password Field Enabled	If enabled, displays a password field on the form.
Password Field Required	If enabled, the user is required to complete this field on the form.
Password Field Label	Text label for password field on the form.

Setting	Definition
Password Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Password Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
First Name Field Enabled	If enabled, displays a First Name field on the form.
First Name Field Required	If enabled, the user is required to complete this field on the form.
First Name Field Label	Text label for the First Name field on the form.
First Name Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
First Name Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Last Name Field Enabled	If enabled, displays a Last Name field on the form.
Last Name Field Required	If enabled, the user is required to complete this field on the form.
Last Name Field Label	Text label for the Last Name field on the form.
Last Name Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Last Name Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Security and Access Value (S&A) Field Enabled	If enabled, displays a field for the Security and Access Value on the form.
S&A Field Required	If enabled, the user is required to complete the Address field on the form.
S&A Field Label	Text label for the S&A field on the form.

Setting	Definition
S&A Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
S&A Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Role Field Enabled	If enabled, network access is limited based on the Role Name in the Role Field Value field and the roles created under Go - Manage - Roles. Roles provide location-based access control.
Role Field Required	If enabled, this field must be completed to submit the form.
Role Field Label	Text label for the Role field on the form.
Role Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Role Field Value	Data entry field used to submit data with the form. Requires a role name. Roles are used to control network access. Typically this field is set by the administrator with the field type set to hidden. Role names must match those in the database. You can also create a list of roles for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green.
Title Field Enabled	If enabled, displays a field for the user's title on the form.
Title Field Required	If enabled, the user is required to complete this field on the form.
Title Field Label	Text label for the title field on the form.
Title Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Title Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Address Field Enabled	If enabled, displays a field for the user's address on the form.
Address Field Required	If enabled, the user is required to complete the Address field on the form.
Address Field Label	Text label for the Address field on the form.

Setting	Definition
Address Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Address Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
City Field Enabled	If enabled, displays a field for the user's city on the form.
City Field Required	If enabled, the user is required to complete this field on the form.
City Field Label	Text label for the City field on the form.
City Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
City Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
State/Province Field Enabled	If enabled, displays a State/Province field on the form.
State/Province Field Required	If enabled, the user is required to complete this field on the form.
State/Province Field Label	Text label for the State/Province field on the form.
State/Province Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
State/Province Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Postal Code Field Enabled	If enabled, displays a Postal Code field on the form.
Postal Code Field Required	If enabled, the user is required to complete this field on the form.
Postal Code Field Label	Text label for the Postal Code field on the form.

Setting	Definition
Postal Code Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Postal Code Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Email Field Enabled	If enabled, displays a field for the user's e-mail on the form.
Email Field Required	If enabled, the user is required to complete this field on the form.
Email Field Label	Text label for the e-mail field on the form.
Email Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Email Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Phone Field Enabled	If enabled, displays a telephone number field on the form.
Phone Field Required	If enabled, the user is required to complete this field on the form.
Phone Field Label	Text label for the telephone number field on the form.
Phone Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Phone Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Hardware Description Field Enabled	If enabled, displays a field for to describe the user's hardware on the form.
Hardware Description Field Required	If enabled, the user is required to complete this field on the form.
Hardware Description Field Label	Text label for the hardware description field on the form.

Setting	Definition
Hardware Description Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Hardware Description Field Value	Data entry field provided for user. You have the option to enter a default value for the field that can be overridden by the user or a list of items for selection. If the field type is set to hidden, you can submit a hidden value with the form.
Serial Number Field Enabled	If enabled, displays a field for the serial number of the user's PC or other device on the form.
Serial Number Field Required	If enabled, the user is required to complete this field on the form.
Serial Number Field Label	Text label for the field containing the serial number of the user's PC or other device on the form.
Serial Number Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Serial Number Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Hostname Field Enabled	If enabled, displays a field for the name of the user's PC or hostname on the form.
Hostname Field Required	If enabled, the user is required to complete this field on the form.
Hostname Field Label	Text label for the field containing the name of the user's PC or hostname on the form.
Hostname Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Hostname Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.

User login (in-line only)

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being

Setting	Definition
	used, the title also displays on the appropriate tab.
Title	Text title for the first paragraph in the login page. Displays above the text entered in the Introduction property.
Left Column Content	Text displayed in the left column of the page.
Introduction	Text displayed in the first paragraph of the regular network user login page.
Secondary Text	Text displayed in the second paragraph of the regular network user login page.
Instructions	Select whether instructions will be included in this page, as a link to Instructions, or not at all. Instruction are entered in the Content Editor under VPN-Instructions.

User login form (in-line only)

Setting	Definition
Form Title	Text label displayed at the top of the login form.
Form Action	Redirects the user to the next page in the sequence.
	 Changing the form action to an unsupported page may affect functionality.
Success Page (Relative)	Relative URL to the success message.
	 Changing this may affect supported functionality.
Missing Fields Message	Message displayed to the user if all required fields on the form are not completed.
Host Expiration Period Enabled	If enabled, the amount of time that the host can access the network is limited to the time entered in the Host Expiration Period Value field. The Host Expiration Period Value field defaults to hidden. The time value provided by the Administrator and is submitted with the rest of the form data.
Host Expiration Period Unit	The Unit of measurement for the amount of time that the host will be registered before expiry.
Host Expiration Period Value	The amount of time that the host will be registered before expiry.
Username Field Enabled	If enabled, displays a Username field on the form.
Username Field Required	If enabled, the user is required to complete this field on the form.
Username Field Label	Text label for the Username field on the form.

Setting	Definition
Username Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Username Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Password Field Enabled	If enabled, displays a password field on the form.
Password Field Required	If enabled, the user is required to complete this field on the form.
Password Field Label	Text label for password field on the form.
Password Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Password Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
First Name Field Enabled	If enabled, displays a First Name field on the form.
First Name Field Required	If enabled, the user is required to complete this field on the form.
First Name Field Label	Text label for the First Name field on the form.
First Name Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
First Name Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Last Name Field Enabled	If enabled, displays a Last Name field on the form.
Last Name Field Required	If enabled, the user is required to complete this field on the form.
Last Name Field Label	Text label for the Last Name field on the form.

Setting	Definition
Last Name Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Last Name Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Security and Access Value (S&A) Field Enabled	If enabled, displays a field for the Security and Access Value on the form.
S&A Field Required	If enabled, the user is required to complete the Address field on the form.
S&A Field Label	Text label for the S&A field on the form.
S&A Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
S&A Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Role Field Enabled	If enabled, network access is limited based on the Role Name in the Role Field Value field and the roles created under Go - Manage - Roles. Roles provide location-based access control.
Role Field Required	If enabled, this field must be completed to submit the form.
Role Field Label	Text label for the Role field on the form.
Role Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Role Field Value	Data entry field used to submit data with the form. Requires a role name. Roles are used to control network access. Typically this field is set by the administrator with the field type set to hidden. Role names must match those in the database. You can also create a list of roles for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green.
Title Field Enabled	If enabled, displays a field for the user's title on the form.
Title Field Required	If enabled, the user is required to complete this field on the form.
Title Field Label	Text label for the title field on the form.

Setting	Definition
Title Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Title Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Address Field Enabled	If enabled, displays a field for the user's address on the form.
Address Field Required	If enabled, the user is required to complete the Address field on the form.
Address Field Label	Text label for the Address field on the form.
Address Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Address Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
City Field Enabled	If enabled, displays a field for the user's city on the form.
City Field Required	If enabled, the user is required to complete this field on the form.
City Field Label	Text label for the City field on the form.
City Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
City Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
State/Province Field Enabled	If enabled, displays a State/Province field on the form.
State/Province Field Required	If enabled, the user is required to complete this field on the form.
State/Province Field Label	Text label for the State/Province field on the form.

Setting	Definition
State/Province Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
State/Province Field Value	Data entry field provided for the user. You have the option to enter a default value for the field that can be overridden by the user or a list of items for selection. If the field type is set to hidden, you can submit a hidden value with the form.
Postal Code Field Enabled	If enabled, displays a Postal Code field on the form.
Postal Code Field Required	If enabled, the user is required to complete this field on the form.
Postal Code Field Label	Text label for the Postal Code field on the form.
Postal Code Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Postal Code Field Value	Data entry field provided for the user. You have the option to enter a default value for the field that can be overridden by the user or a list of items for selection. If the field type is set to hidden, you can submit a hidden value with the form.
Email Field Enabled	If enabled, displays a field for the user's e-mail on the form.
Email Field Required	If enabled, the user is required to complete this field on the form.
Email Field Label	Text label for the e-mail field on the form.
Email Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Email Field Value	Data entry field provided for user. You have the option to enter a default value for the field that can be overridden by the user or a list of items for selection. If the field type is set to hidden, you can submit a hidden value with the form.
Phone Field Enabled	If enabled, displays a telephone number field on the form.
Phone Field Required	If enabled, the user is required to complete this field on the form.
Phone Field Label	Text label for the telephone number field on the form.
Phone Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.

Setting	Definition
Phone Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Hardware Description Field Enabled	If enabled, displays a field for to describe the user's hardware on the form.
Hardware Description Field Required	If enabled, the user is required to complete this field on the form.
Hardware Description Field Label	Text label for the hardware description field on the form.
Hardware Description Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Hardware Description Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Serial Number Field Enabled	If enabled, displays a field for the serial number of the user's PC or other device on the form.
Serial Number Field Required	If enabled, the user is required to complete this field on the form.
Serial Number Field Label	Text label for the field containing the serial number of the user's PC or other device on the form.
Serial Number Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Serial Number Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.
Hostname Field Enabled	If enabled, displays a field for the name of the user's PC or hostname on the form.
Hostname Field Required	If enabled, the user is required to complete this field on the form.
Hostname Field Label	Text label for the field containing the name of the user's PC or hostname on the form.

Setting	Definition
Hostname Field Type	Indicates the control type for this field. Types include: Input-text field. Select-a drop-down list of preset options. Hidden-field submitted with the form but is hidden from the user. Password-text that is masked by asterisks or dots as it is typed.
Hostname Field Value	Data entry field provided for the user. You have the following options for the field. Enter a default text value for the field that can be overridden by the user. Create a list of items for selection using the following syntax (Value,Name : Value,Name). Example: Color1,Blue : Color2,Red : Color3:Green. If the field type is set to hidden, you can submit a hidden value with the form.

Profile configuration download

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Left Column Content	Text displayed in the left column of the page.
Introduction	Introductory text explaining what steps need to be taken.
Download Link Prefix	Text displayed before the download link.
Download Link	Text displayed as a link.
Download Link Suffix	Text displayed after the download link.
Button Text	Text displayed on the button on the profile download page.

Mobile Agent download

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Left Column Content	Text displayed in the left column of the page.
Introduction	Introductory text explaining what steps need to be taken.
Download Link Prefix	Text displayed before the download link.
Download Link	Text displayed as a link.
Download Link Suffix	Text displayed after the download link.

Instructions

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.

Setting	Definition
Title	Title displayed above the Introduction property contents.
Left Column Content	Text displayed in the left column of the page.
Introduction	Text introduction to the instructions page.
Show Windows Instructions	If enabled, display instructions for computers running Windows.
Windows Instructions	Instructional text for computers running Windows.
Show macOS Instructions	If enabled, display instructions for computers running macOS.
macOS Instructions	Instructional text for computers running macOS.
Show Linux Instructions	If enabled, display instructions for computers running Linux.
Linux Instructions	Instructional text for computers running Linux.
Show Other Instructions	If enabled, display instructions for other computers.
Other Instructions Title	Title of the instructions for other computers.
Other Instructions	Instructional text for other computers.
Display as Accordion View	Use JavaScript to display the instructions as an accordion.

Success

Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title displayed above the Success Message contents.
Left Column Content	Text displayed in the left column of the page.
Please Wait Message	Message displayed to the user while the progress bar moves. To change the amount of time the message and progress bar are displayed, modify the default 45 second countdown number.
Progress Bar Enabled	If checked, display a progress bar and display the finished message.
Progress Bar Title	Text title displayed above the progress bar.
Finished Message	Message displayed to the user when the progress bar has finished.
Success Message	Message displayed upon successful connection.

Agent

Configure the settings and behavior of agents.

Mobile

Setting	Definition
Message	Text displayed in the middle of the screen.
Username Hint	Text displayed as a hint in the user name field.
Password Hint	Text displayed as a hint in the password field.
Button Text	Text displayed in the registration button.
Authenticate Mobile Hosts	If enabled, authenticate registered hosts.

Dissolvable

Setting	Definition
Results Text	Text displayed above the results list.
Login Type Label	Text displayed as the first option in the login type box.
Connection test URL	A publicly accessible URL that is otherwise blocked from an isolation VLAN. When the agent receives a 200 response while attempting to connect to the URL, the success message appears.
Skip Message Screen	When enabled, automatically starts the Dissolvable agent without displaying the initial message screen. Requires Agent version 4.0.5 and higher.
Message	Text displayed in the middle of the screen.
Username Hint	Text displayed as a hint in the user name field.
Password Hint	Text displayed as a hint in the password field.
Button Text	Text displayed in the registration button.
Rescan Button Text	Text displayed in the rescan button.
Cancel Button Text	Text displayed in the Cancel button.
Finish Button Text	Text displayed in the Finish button.
EasyConnect Login Dialog Title	Text displayed as the title for the Dissolvable Agent Login dialog. Requires agent version 3.3 or higher.
EasyConnect Login Dialog Message	Text displayed when the Dissolvable Agent prompts for credentials. Requires agent version 3.3 or higher.
Success Text	Text displayed after a successful registration.
Skip Success Screen	When enabled, closes the agent without displaying the success screen. Requires Agent version 4.0.5 and higher.
Launch Success Page	Select to launch the success page after the user clicks Finish.

EasyConnect

Provides a button to run EasyConnect through the Persistent Agent, allowing the EasyConnect process to run again if the secure wireless configuration on a device has changed.

Requires agent version 3.3 or higher.

Run EasyConnect

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title displayed above the Success Message contents.
Left Column Content	Text displayed in the left column of the page.
Content	Text displayed in the web page.
Button Text	Text displayed on the button to re-run EasyConnect.
Retry Text	Text displayed on the Retry button.
Validating Persistent Agent Message	Text displayed while system communicates with Persistent Agent.
Validating EasyConnect Policy Message	Text displayed while system searches for EasyConnect policy.
Policy Matched Message	Text displayed when the EasyConnect policy is found.

Success

Setting	Definition
Window Title	Text label displayed in the title of the browser window. If multiple tabs are being used, the title also displays on the appropriate tab.
Title	Text title displayed above the Success Message contents.
Left Column Content	Text displayed in the left column of the page.
Success Message	Message displayed upon successful connection.
Finished Message	Message displayed to the user when the progress bar has finished.
Progress Bar Enabled	If checked, display a progress bar and display the finished message.
Please Wait Message	Message displayed to the user while the progress bar moves. To change the amount of time the message and progress bar are displayed, modify the default 45 second countdown number.
Progress Bar Title	Text title displayed above the progress bar.

Copy a portal

1. Select **Portal > Portal Configuration**.
2. Click on the **Content Editor** tab.
3. Click the **Copy** button.
4. Use the following table to select options:

Field	Definition
Copy Only Style Information	If enabled, copies only the Styles and Custom Rule Definitions configured under Global > Styles . If disabled, all elements are copied from the selected portal to the portal designated in the Portal Name field.
Copy Into An Existing Portal	If enabled, the Portal Name field becomes a drop-down list of existing portals. Elements from the portal selected on the Content Editor tab are copied to the portal selected in the drop-down list.
Portal Name	Name of the portal to which elements of another portal will be copied. If Copy Into an Existing Portal is disabled, a new portal is created. If Copy Into an Existing Portal is enabled, this field is a drop-down list of existing portals and the selected portal is updated.

5. Click **OK** to copy the portal.

Select a default portal

Select a default portal to be used if FortiNAC cannot determine the portal that should be presented to a user in an environment where there are multiple portals.

1. Select **Portal > Portal Configuration**.
2. Click on the **Content Editor** tab.
3. Select the portal that will be the default portal.
4. Click the **Set as Default** button.
5. In the list of portals, the default portal is shown at the top of the list.

Delete a portal

If any portal policies use the portal configuration being deleted, those policies are also deleted.

1. Select **Portal > Portal Configuration**.
2. Click on the **Content Editor** tab.
3. Locate the portal you want to delete and click the delete button
4. A confirmation message is displayed. Click **Yes** to continue.

Images

Use the Images tab on the Portal Configuration view to upload and preview images for the portal configuration selected on the Content Editor tab.

Max image size = 1MB

1. Select **Portal > Portal Configuration**.
2. Click on the **Images** tab.
3. To preview an image, select it and click the preview button. The image displays in the panel on the right.
4. To upload an image, click the **Upload Images** button.
5. Browse to the image you want to upload and click **Open**.
6. Scroll through the list to make sure your image was uploaded.

Version 1 settings

Version 1 settings tab allows you to configure the how portal pages appear in the web browser if you are using legacy portal pages.

This tab is only available if **Use Portal Version 1** is enabled on the Portal Configuration view. It controls which portal pages are used when network users log onto your network. Portal Version 1 represents existing portal pages created when you originally set up FortiNAC. Disabling the Portal Version 1 pages enables pages that are distributed with FortiNAC that can be edited using the Content Editor.

Properties Settings in this window include:

- **Labels** — Displays a text label below the portal page header.
- **Images** — Displays an image in the portal page header at the top of the page.
- **Links** — Specifies a web page that displays in the browser when the login credentials are successfully authenticated.

Settings

Field	Definition
Portal Settings	
Web Page Label	Banner that displays at the top of the portal page when a user attempts to connect to the network.
Web Page Footer	Text that displays across the bottom of the portal page when a user attempts to connect to the network.
Upload Image Button	Browse for and upload an image to display on the portal page.
Home Page URL for Successful Registration	URL to which the users are directed when they have successfully registered. Copy this URL into a browser to verify that the correct page is displayed.
Resolve URL button	Resolves the IP of the URL selected for the Home Page.
Standard User Authentication	

Field	Definition
Authentication Type	Valid users are allowed to access certain network areas on a regular basis. Choose from three authentication types: Local—Validates the user to a database on the local FortiNAC appliance. LDAP—Validates the user to a directory database. FortiNAC uses the LDAP protocol to communicate to an organization's directory. See Directories on page 868 for configuration information. RADIUS—Validates the user to a RADIUS server.  PAP encryption must be set up on the RADIUS server for encryption/decryption of user names and passwords that are sent to and from FortiNAC, such as the user name and password for the Validation Account used for communication between FortiNAC and the RADIUS server.



If you are not using Version 1 Portal Pages, authentication type is set in the Content Editor under **Global > Settings > Standard User Authentication Type**.

1. Select **Portal > Portal Configuration**.
2. Click the **Version 1 Settings** tab. This tab is only displayed if the Use Portal Version 1 option is enabled on the Portal Configuration view.
3. Under the Portal Settings section, enter a text label into the **Web Page Label** field. This label displays below the header image on your portal pages. Typically, this is the name of the company or organization.
4. Enter a text label into the **Web Page Footer** field. This label displays at the bottom of your portal pages, such as "For assistance, contact the help desk."
5. To display an image on your portal page, click the **Upload Image** button. Navigate to the image file and select it.
6. To specify a web page for successful registration, enter a URL in the **Home Page URL for Successful Registration** field.



Cut and paste the link into a browser to verify that the URL directs you to the correct page.

7. Click the **Resolve URL** button. The URL resolves to an IP. The IP address of the URL is entered into the field.
8. The Standard User Authentication section determines how users are authenticated.
9. Click **Apply**.

Enable the common account



The Common Account is only available if the **Use Portal Version 1** option is enabled on the Portal Configuration view. The Common Account can only be used with legacy portal pages.

Allows you to configure a generic or common account for visitors. If you check Enable in the Common Account section, visitors view a different login screen and do not enter a user name and password. The visitor enters only predefined information, such as first name, last name, telephone number, and so on. To be authenticated, the visitor uses the default user name and password that you specify in the Common Account section.

Configure the following parameters for Common accounts:

- **Enable** — Enables default user name and password for guest access.
- **User Name** — Specifies a default user name for the default guest account. You may choose a user name such as *defaultguest* to easily identify the statistics of all default guests.
- **Password** — Specifies a default password for the default guest accounts. The guest does not enter this password. FortiNAC uses this password internally to authenticate the guest to an existing user entry.

1. Select **Portal > Portal Configuration**.
2. Click on the **Version 1 Settings** tab.
3. In the Common Account section of the window select the **Enable** check box.
4. Enter a default user name into the **User Name** field.
5. Enter a default password into the **Password** field.
6. Click **Apply**.

Reserved portal page file names

If you choose to create your own pages for the portal, you must avoid using any of the following file names. Files with the names listed below are used by FortiNAC for the pages distributed with the program. These files should never be modified outside of the Portal Configuration Content Editor. Future upgrades could overwrite those changes.

-
• AgentDownload2.jsp	• index-remediation.jsp
• CustomLogin.jsp	• index-vpn.jsp
• Disagree.jsp	• Instructions.jsp
• Error.jsp	• LoginMenu.jsp
• ExternalLogOff.jsp	• LogOff.jsp
• Fail.jsp	• LogOffSuccess.jsp
• FailureInfo.jsp	• Policy.jsp
• FindMac.jsp	• PortalIndex.jsp
• GameRegister.jsp	• RemoteScan.jsp
• GuestLoginGCS.jsp	• RemoteSuccess.jsp
• index-authentication.jsp	• RemRedirect.jsp
• index-deadEnd.jsp	• Success.jsp
• index-hub.jsp	• ValidUserLogin.jsp
• index-registration.jsp	• VPNLogin.jsp
-

Anything starting with portalCommon should be avoided.

portalCommon/**

Configure authentication credentials

Authentication Credentials for Standard Users are configured in the Portal Configuration Content Editor tab under **Global > Settings > Standard User Authentication Type**. If Portal Version 1 is enabled, Authentication Credentials are configured on the Version 1 Settings tab. These options control how the system validates user credentials for the following login categories:

- **Standard Users**—Users that are assigned their own user names and passwords for logging onto the network on a regular basis. These users might include employees, students, and administrators.
- **Common Account**—Generic account that does not require guests to enter a user name and password, if enabled. Available for Portal Version 1 Only.

The Common Account option is only available for appliances with firmware images 2.2.0.x through 2.3.2.x.

The Version 1 Settings tab is only available if the Use Portal Version 1 option is enabled on the General tab of the Portal Configuration window.

Authenticate standard users

Valid users are allowed to access certain network areas on a regular basis. Authentication type is set differently depending on the configuration of your portal pages. Typically, authentication type is set through the Content Editor under **Global > Settings > Standard User Authentication Type**. If you have enabled the Use Portal Version 1 option on the Portal Page Configuration window, authentication is set on the Version 1 Settings tab of that window.

If you are using the Persistent Agent to scan hosts against security policies, the authentication method selected for the Persistent Agent must match the authentication method selected here. See [Credential configuration on page 918](#).

Authentication types include:

- **Local** — Validates the user to a database on the local FortiNAC. Use this option if you plan to enter a list of registered users.
- **Local/Device** — Validates the user, but registers the host as the device with no owner.
- **LDAP** — Validates the user to a directory database. FortiNAC uses the LDAP protocol to communicate to an organization's directory.
- **LDAP/Device** — Validates the user to a directory database, but registers the host as the device with no owner.
- **RADIUS** — Validates the user to a RADIUS server. PAP encryption must be set up on the RADIUS server for encryption/decryption of user names and passwords that are sent to and from FortiNAC, such as the user name and password for the Validation Account used for communication between FortiNAC and the RADIUS server.
- **RADIUS/LDAP** — Validates the user to a RADIUS server, but registers the user based on data contained in an LDAP server. If the user is successfully authenticated by the RADIUS server but does not exist in the LDAP database, FortiNAC will still create the user record in its own database.
- **RADIUS/Device** — Validates the user to a RADIUS server, but registers the host as a device with no owner.
- **HTTP User** — Delegates user validation to HTTP Authentication. Registers to, creating if necessary, a user in the local FortiNAC database.
- **HTTP User/LDAP** — Delegates the user validation to HTTP Authentication, but registers the user based on data contained in an LDAP server. If the user is successfully authenticated but does not exist in the LDAP database, FortiNAC will still create the user record in its own database.
- **HTTP User/Device** — Delegates user validation to HTTP Authentication, but registers the host as a device with no owner.
- **Google** — Requires Agent 3.3 and above. Enables the user to log in with a Google account.

- **Google/Device** — Requires Agent 3.3 and above. Enables the user to log in with a Google account, but registers the host as a device with no owner.
- **None/Device** — Requires Agent 3.3 and above. Allows user to register without a username and password. Registers the host as a device with no owner.

Assign an authentication type

1. Select **Portal > Portal Configuration**.
2. If Use Portal Version 1 is not enabled, click on the **Content Editor** tab.
3. If you have created more than one portal, select the portal to be edited from the drop-down list at the bottom of the view.
4. Click the **Global** option in the tree on the left to expand it. Under Global, select **Settings**. In the pane on the right locate the **Standard User Authentication** field and select **Local**, **LDAP**, **RADIUS**, **RADIUS/LDAP**, **HTTP User** or **HTTP User/LDAP** from the drop-down menu.
5. In the tree on the left select **Registration > Login Menu**. Make sure that **Standard User Login** is enabled.
6. Click **Apply**.

Example - change portal image

The steps outlined in this example lead you through uploading an image, adding a banner to your web pages, including an image as the background for the banner and resizing the page.

Upload an image

First you must upload the image you wish to use as the background for your banner. Both the width of the banner and the width of the base page can be adjusted using the style editor. For this example, we will assume that the width needed is 780 pixels. The banner image uploaded would need to be 780 pixels.

1. Select **Portal > Portal Configuration**.
2. Click on the **Content Editor** tab.
3. If you have created more than one portal, select the portal to be edited from the drop-down list at the bottom of the view.
4. Click on the **Images** tab.
5. To preview an image, select it and click the preview button. The image displays in the panel on the right.
6. To upload an image, click the **Upload Images** button.
7. Browse to the image you want to upload and click **Open**.
8. Scroll through the list on the left to make sure your image was uploaded.

Create a banner with an image background

To create the Banner you will have to use the Custom Rules option at the bottom of the Style Sheet Editor to expand the banner from a height of 0 pixels to an appropriate size. In this example, we are setting the banner to 80 pixels by 780 pixels. We will also adjust the page width to 780 pixels.

To use Custom Rules you must have a working knowledge of CSS.

1. Select **Portal > Portal Configuration**.
2. Click on the **Content Editor** tab.

3. Select the portal to be edited, and click edit button.
4. Navigate to the styles tab.
5. Scroll to the **Custom Rules Definitions** section at the bottom of the window. Using the Custom Rules option you can add multiple rules and each rule can contain multiple properties.
6. Click **Add Rule**.
7. In the field containing **Enter Selector**, type *.branding*.
8. In the field containing **Enter Property**, type *height*.
9. In the field containing **Enter Value**, type the height of your image, such as *80px*.
10. Click **Add Property** to add the next property which is the width of the image.
11. In the **Property** field, enter *width*.
12. In the **Value** field enter the width of the image, such as *780px*. Click **Add Property** to add the next property which is the background image.
13. In the Property field enter *background-image*.
14. In the Value field enter *url('../img/imagename.jpg')* where imagename.jpg is the name of the image you uploaded earlier. If you would like to test this with a sample image, use *banner.jpg*.
In order to display uploaded images, the path to the image directory must be included in the Value field as follows:
`../ ../img/`
15. Click **Add Rule**.
16. In the field containing **Enter Selector** type *#custom-doc*.
17. In the **Property** field, enter *width*.
18. In the **Value** field, enter the width of the page, such as *780px*. Now the page and the banner will be the same width.
19. Click **Apply** to save.

Disable captive portal

In certain situations, you may need to disable the captive portal to restrict network access for all users. There are two available methods to disable the captive portal.

Method 1: Layer 3 Option

1. Navigate to **System > Config Wizard > Basic Network**.
2. Under **Network Type**, select **None: Don't configure Isolation Networks**.

Network Type

Please select the type of network you are configuring:

☒ None: Don't configure Isolation Networks

☐ Layer 3 network: Routed Network with multiple scopes for each isolation network.
Select Layer 3 when the Isolation Networks are separated from the FortiNAC Appliance by a router or the host VLANs can not be trunked back to the FortiNAC appliance. In this case the Host VLANs will route back to the network appliance. The remote Isolation VLANs will utilize IP-Helpers to enable the Hosts to receive DHCP from the FortiNAC appliance.

☐ Layer 2 network: 802.1Q trunking setup with single scope per VLAN/isolation network.
Select Layer 2 when the Isolation Networks will not span across a router, all VLANs can be 802.1q tagged to the FortiNAC appliances interface.

3. Go to the **Summary** tab, and click **Apply** to save changes.

Method 2: Layer 2 Option

- 1. Navigate to **System > Config Wizard > Layer 3 Isolation**.
- 2. Uncheck **Isolation Interface port 2**

Steps

Basic Network

Layer 3 Isolation

Layer 3 Registration

Layer 3 Remediation

Layer 3 Dead End

Layer 3 Virtual Private Network

Layer 3 Authentication

Additional Routes

Summary

Layer 3 Network Configuration

☐ Isolation Interface port2

Interface IPv4 Address

IPv4 Gateway (Optional: used for route creation)

Interface IPv6 Address

IPv6 Gateway (Optional: used for route creation)

Isolation Scopes

☐	Label	Gateway	Mask	Domain
☐	isolation			isol.nacqa.test

- 3. Go to the **Summary** tab, and click **Apply** to finalize the changes.

Request Processing Rules

The FortiNAC application is divided into two primary components, the first being the Administrative components and the second being the End User components. The main portion of the End User side of the application is the Portal. The Portal is a series of customizable web pages that guide the end user, members of the customer's organization, through the process of authenticating, scanning, and registering their device on the network.

As the portal is a web application, clients connect via their browser which sends HTTP requests, but more than just web browsers will send HTTP requests to the Portal. These requests need to be routed through the workflow differently based upon their purpose. Request Processing Rules is a way to control this routing by either blocking, allowing, forwarding, or returning a specific file for any request based on information available in the HTTP request.

Tools

Tool	Description
Create New	The administrator may define a new Request Processing Rule which will be added to the end of the list. Request Processing Rules are ordered automatically in the system when written to the HTTP server to produce the correct result. The changes from adding a rule do not immediately go into effect for the web server, as applying them requires restarting a process.
Edit	Functionally similar to the Create New action, this modifies the existing rule in place. The changes from editing a rule do not immediately go into effect for the web server, as applying them requires restarting a process.
Delete	Following confirmation from the administrator, this action removes one or more selected rules. The changes from deleting a rule do not immediately go into effect for the web server, as applying them requires restarting a process.
Auto Configure	This action brings up an overlay where the user may Enable or Disable detection for the Mac OS X and iOS Captive Network Assistants. The Captive Network Assistant (CNA) is a limited-functionality web view that appears on these operating systems when it detects a captive network. By clicking Enable or Disable, the system attempts to locate the rules which would influence the CNA and modify them so that the CNA either appears or does not appear when a device is placed in isolation. The changes from this do not immediately go into effect for the web server, as applying them requires restarting a process, but the administrator will be immediately presented with the overlay from the Publish action when they click either button. Enabled: when enabled, "apple.com" will be removed from the list of allowed domains, and Apple CNA portal will open automatically. Follow the instruction to copy and paste the URL onto a browser to complete the registration. Please see note below. Disabled: when disabled, "apple.com" will be included in the list of allowed domains, and Apple CNA portal will not open automatically.

Tool	Description
Publish	This action brings up an overlay where the user can write the existing set of Request Processing Rules to the web server and restart the process. This only restarts the HTTP server for the Portal and is generally very quick. Changes are automatically published whenever the FortiNAC process is started, such as after a system reboot or an upgrade. The Publish task will automatically define and order all rules to produce a correct chain of conditionals. The result is outputted to the Application server at <code>/etc/httpd/conf.d/000_web_servces.conf</code>



Auto Configure Note: Apple CNA does not open automatically when a Apple device is connected for host registration due to halt on network traffic on all applications, thus agent will not be accessible to for download.

To remediate this issue, enable **Auto Configure** will prevent Apple CNA from issuing HTTP request, and allow AppleCNA portal to open automatically with instructions on host registration. To edit the AppleCNA Portal registration page, please see [Apple CNA Instructions Portal on page 743](#).

Add or Edit a Rule

1. Navigate to **Portal > Request Processing Rules**
2. Click **Create New** or select an existing entry and click **Edit**
3. Fill out the available settings found below in the table

Settings

Field	Description
Field	The field in the HTTP Request to read the value of when determining if the Action should be taken. Currently supported fields are Request URI and HTTP User Agent. If the value in the Field matches the Matcher, the Action will be taken.
Matcher	A regular expression used to match the value read from the Field. Because this is a regular expression, certain characters have a special meaning, such as dot (.) meaning any character, star (*) meaning 0 or more instances, and backslash (\) being the escape character. See documentation about regular expressions for more information.
Action	The action to take if the Matcher successfully matches the value in the Field. There are four possible actions: Allow, Block, Forward, and File. When selecting Forward and File, the Target value is also required.
Target	Related to the Action, this value contains either the target URL for the Forward action or the target file path for the File action. In the case of the File target, entering only exclamation point (!) has the meaning of loading a file at the same path as the Request URI in the HTTP request.

Additional Rule Descriptors

Field	Description
Last Modified By	The user ID of the last Administrator to modify this entry. If the entry was last modified by an automated process within FortiNAC, the ID listed here is SYSTEM.
Last Modified Date	The date and time that the most recent modification took place. This is a UTC timestamp, so it should appear relative to the end user's timezone as defined in their browser.

Apple CNA Instructions Portal

The purpose of using Apple CNA Instruction to register the Apple device user is to provide workaround when AppleCNA Captive Portal does not open automatically. AppleCNA Captive Portal opens automatically by default when an Apple device is connected to a hotspot and provide instructions to register.

However, AppleCNA Captive Portal prevents Apple devices from registering host on FortiNAC due to network connection issue. The work around is to enable Auto Configure at **Portal > Request Processing Rules**, then Apple CNA Instruction Portal will automatically appear with instruction to copy and paste the registration URL to a browser to finish host registration.



Default instructions

Setting	Definition
Window Title	Text labeled displayed for the title of the browser window.
Title	Text title for the Apple CAN instructions page.
Left Column Content	Text displayed on the left column of the page.
Top Content	Text providing instructions and information on how to register without using Apple Captive Network Assistant.
Copy Button Text	Button to copy text.
Bottom Content	Text after the portal URL that explains how to reach the portal outside of the CAN.

Portal SSL

Use this view to configure the security access level and the fully qualified host name for the portal pages presented to users when their devices or hosts are isolated from the network.

Requires installing SSL certificate to the Portal certificate target. This can be either a certificate from a public or private Certificate Authority (CA) (recommended) or a self-signed certificate. For details, see [Server certificates](#).

Settings

Field	Definition
SSL Mode	Valid SSL Certificate: When web traffic reaches the captive portal, it is redirected from port 80 to port 443 and presents a SSL certificate to the user.
Fully Qualified Host Name	The fully qualified name used for portal access. Can be the fully qualified name of the appliance or some other name. Requirement: Must match the Subject Name or a Subject Alternative Name secured with the SSL certificate installed in the Portal Certificate Target.

Logs

Audit Logs	746
Events	749
Alarms	783
Reports	793
Scan results	804
Security Incidents	806

Audit Logs

The **Audit Logs** log tracks all changes made to an item in the system. Users with admin auditing permissions will see a change in the admin auditing log whenever data or port is added, modified, or deleted. Users can see what was changed, when the change was made, and who made the change.

Changes made through the CLI are tracked in the admin auditing log; however, the user ID for the user who made the change will appear as **CLI Tool**.

Changes can be filtered by the name of the item that was changed, the action taken, the date when the change occurred, the user ID for the user who made the change, and the type of item that was changed.

Changes made to the following items are not currently audited:

- Trap MIB files
- NTP and time zone settings
- Adapters
- RADIUS domain mappings
- RADIUS server defaults
- Security applications
- Alarms
- Certificates
- Portal SSL settings
- Portal configuration styles
- Mobile providers
- Database backup settings (excluding the Backup Timeout)
- Changes to the license key

Changing the name of a device or moving a device to a new container will result in a separate audit entry for each port on the device.

Auditing archives and purges audits made to hosts, users, or elements.

Configuration

Users must have permission to view the auditing log.

1. Click **Users & Hosts > Administrators > Profiles**.
2. Click **Add** or select an administrator profile and click **Modify**. (Note: The permissions for the System Administrator profile cannot be changed).
3. Click **Permissions** tab.
4. Select the **Access** check box next to **Admin Auditing**.
5. Click **OK**.

Accessing the auditing log

1. Click **Logs > Audit Logs**.
2. Click a row to view the entire list of changes in **Change Details** window below.

Add/Modify Filter

1. Hover cursor over the column header. A filter icon will display.
2. Click the filter icon. A window appears with the applicable parameters. See Settings Table below for possible parameters.
3. Select the desired filter operation (range, exact match, etc).
4. Select all criteria desired to search. For filters that include a search field, either manually enter or click the desired values to search.
Note: Multiple Values can be OR'd together. If manually entering, use either "," or "]" between values. Otherwise, click all desired values in the below window.
5. Click **Apply**.

Delete Filter

1. Click filter icon in column header
2. Click **Remove**.

Settings

Field	Definition
Add Filter	Allows you to select a field from the current view to filter information. Select the field from the drop-down list, and then enter the information you wish to filter. See Filters on page 34 .
Update	Displays the filtered data in the table.
Admin auditing	
Date	The date and time when the change was made. Filter Operations: "=", Range, "<=", ">=", NOT
User ID	The user ID of the user who made the change. The user ID appears as "CLI Tool" when changes are made using CLI tools.

Field	Definition
	Filter Operations: Contains, Exact Match, NOT
Action	Shows whether the change involved adding, modifying, or deleting information. Filter Operations: Contains, Exact Match, NOT
Type	The type of item that was changed. Filter Operations: Contains, Exact Match, NOT
Name	The name of the item that was changed. Click the name to view a dialog containing all changes that have been made to the area. Filter Operations: Contains, Exact Match, NOT
Summary	The first four lines of what was changed on the specified date. Filter Operations: None
Change Details	Displays all details of the change made to the item on the specified date. This information appears when you click a row representing a change in the Admin Auditing table.

Events

Events displays the contents of the events log. The events log is an audit trail of significant network and FortiNAC incidents. Events are logged when they are enabled in the events management view. See [Enable and disable events on page 773](#).

To access events, go to **Logs > Events & Alarms > Events**.

Settings

Field	Definition
First Name	First Name of the user associated with the event, such as the registered owner of a host or an administrator.
Last Name	Last Name of the user associated with the event.
Login Name	User name from the credentials of the user who was logged in and associated with the event.
Element Name	Name of the device, administrator, server or process associated with the event.
Element Type	Type can be Device, Port, Container, Process, or All.
Group	Group name of a group of elements, such as port group, device group or user group.
Pause	If enabled, prevents the Events List from refreshing and adding new records to the screen. In an environment with a large number of events, you may need to pause the refresh in order to research an issue.
Date	Date and time that the event occurred.
Event	Event name. See Events and alarms list on page 750 .
Element	Element associated with the event, such as a user, administrator, device, port, or process.
Message	A textual description of the selected entry.
Note	An area for user notes.
Buttons	
Import	Import historical events from an Archive file. See Import archived data on page 102 .
Set Note	Opens a notes window and allows you to add notes to the selected event. See Event notes on page 749 .

Event notes

You can add notes to an event entry to clarify why the event happened, track the resolution of a problem, or add general information.

1. Select **Logs > Events & Alarms > Events**.
2. Use the filters to locate the appropriate event. Refer to [Events on page 749](#) for settings.
3. Select the event.
4. Click **Set Note**.
5. Enter the note text or modify the existing note.
6. Click **OK**.
7. The note text appears on the **Notes** column on the **Events View**.

Events and alarms list

When events are enabled, they can be enabled for All Groups or for a single group. Depending on the event you may not want to enable it for all groups because the volume of events would be overwhelming. For example, if you enabled the host connected event for all groups, you would receive an event message every time someone connects to the network.

When you look at an event in the Event Viewer, additional information is provided about that occurrence of the event. It might include information such as user name, IP address, MAC address or location.

Each event has a corresponding alarm that can be configured. See [Map events to alarms on page 784](#).

Event names highlighted in gray are no longer used. However, they are still available in the Event Log to accommodate importing older data that may contain those events.

Event and Alarm logs can be exported in CSV, XLS, PDF, and RTF formats. Got to **Logs > Events & Alarms**, next to "Export to:" and click on one of the file type to export.

Events and alarms

Event	Definition
Access Configuration Modified	Generated whenever an Access Configuration is modified.
Access Policy Modified	Generated whenever an Access Policy is modified.
Adapter Created	Generated whenever an adapter is added to a host.
Adapter Destroyed	Generated whenever an adapter is removed from a host.
Adapter Connected to a disallowed SSID Adapter Disconnected from disallowed SSID	Adapter connected to/disconnected from SSID not included in the list defined under Restrict Wireless Connections to Specific SSIDs. See Create or edit a configuration . See also KB article https://community.fortinet.com/t5/FortiNAC/Technical-Tip-SSID-AP-check-and-Multihome-detection-with/ta-p/282330
Add/Modify/Remove Blocking via REST API	Generated whenever a REST API request is received that creates or removes a Control Task.
Add/Modify/Remove Host	Generated whenever a trap is received that adds, modifies or removes a host record in the database.
Add/Modify/Remove Host via REST API	Generated whenever a REST API request is received that adds, modifies or removes a host record in the database.

Event	Definition
Add/Modify/Remove User	Generated whenever a trap is received that adds, modifies or removes a user record in the database.
Add/Modify/Remove User via REST API	Generated whenever a REST API request is received that adds, modifies or removes a user record in the database.
Admin User Created	Administrative user created. User types are not included in the event message.
Admin User Destroyed	Administrative user deleted from the database.
Admin User Logged Out	Administrative user logged out of the user interface.
Admin User Login Failure	Administrative user failed to log into the user interface.
Admin User Login Success	Administrative user logged into the user interface.
Admin User Timed Out	Administrative user was logged out of the User Interface based on the settings in Users & Hosts > Administrators > Timeout Settings in the Administrative Interface Inactivity Time (Minutes) field.
Admin Profile Modified	Generates when the Admin Profile has been changed. Reports user and the change made to the profile.
Administrative Status Success	User has gone into port properties for an individual port and successfully turned the Admin Status on or off.
Agent - Unrecognized Vendor OUI	No longer used. Generated when an agent scans a host and returns MAC addresses that have a vendor OUI that is not included in the vendor OUI Management list in FortiNAC.
Agent Message Sent	Message sent from FortiNAC user to one or more hosts. Only hosts running the Persistent Agent can receive messages. This event is not generated if the message fails to send.
Agent Update Failure Agent Update Success	Indicates whether or not an agent updated successfully.
Alarm Created	Indicates that an event has caused an alarm.
Appliance Weak Password(s)	Indicates that password for the appliance and/or the admin UI are either a default factory password or are not complex enough. It is recommended that you modify the password. Otherwise, your network may be at risk for a security breach.
Application Server Contact Lost	Generated when contact is lost to the Nessus plugin in a 1200/8200 pair. Requires contact to be established before contact can be lost.
Application Violation	FortiNAC can receive traps from external applications hosted on servers modeled in the Topology as Pingable or Server devices. This event is generated when a trap is received. Traps might be used to indicate intrusion or that a threshold has been exceeded. A Host Application Violation event can be generated at the same time.

Event	Definition
Application Violation Reset	Generated based on a trap sent from an external application. Indicates that the condition that caused the Application Violation event is no longer happening and operations can return to normal. For example, if hosts have been marked at risk, they can now be marked safe and can access the network. A Host Application Violation Reset can be generated at the same time with host specific information.
Authenticated User	Successfully verified users credentials with the directory.
Authentication Configuration Modified	Generated whenever an authentication configuration is modified.
Authentication Failure	Unable to verify users credentials with the directory.
Authentication Policy Modified	Generated whenever an authentication policy is modified.
Authentication Time-out Failure	User did not authenticate within the allotted time.
Authentication Trap Receive	Received an authentication trap from the directory.
Auto-Definition Synchronizer Failure	FotiNAC unable to perform Auto-Definition update with fnac-updates.fortinet.net.
Auto-Definition Synchronizer Success	FotiNAC successfully performed Auto-Definition update with fnac-updates.fortinet.net.
BigFix High Violation BigFix Medium Violation BigFix Low Violation	Endpoint violation reported by BigFix. For details see Patch management .
Certificate Expiration Warning	Generated when a certificate is due to expire within 30 days.
Certificate Expiration Warning (CRITICAL)	Generated when a certificate is due to expire within 7 days.
Certificate Expired	Generated when a certificate has expired.
cipSecTunnelStop	Generated when VPN connection IPsec Phase-2 Tunnel becomes inactive.
CLI Configuration Failure CLI Configuration Success	Generated when a user tries to configure a Scheduled task that involves applying a CLI configuration to a group. Indicates whether or not the configuration of the scheduled task was successful.
CLI Data Substitution Failure	Indicates failure to substitute the "Port, VLAN, IP, or MAC" data into the CLI.
Communication Lost with BigFix Server	Event indicates that the BigFix patch management server cannot be reached.
Communication Lost with iboss	If configured FortiNAC sends user ID and IP address to iboss each time a host connects to the network. Event indicates that the iboss SSO Agent modeled in the Inventory cannot be reached.

Event	Definition
Communication Lost with Palo Alto User Agent	Palo Alto User Agent is a component of the Palo Alto Firewall. If configured FortiNAC sends user ID and IP address to the Palo Alto User Agent each time a host connects to the network. Event indicates that the Palo Alto User Agent modeled in the Inventory cannot be reached.
Communication Lost with PatchLink Server	Event indicates that the PatchLink patch management server cannot be reached.
Communication Lost with RADIUS/SSO Agent	Fortinet SSO Agent is a component of the FortiGate Firewall. If configured FortiNAC sends user ID and IP address to the Fortinet SSO Agent each time a host connects to the network. Event indicates that the Fortinet SSO Agent modeled in the Inventory cannot be reached.
Communication Lost with Script	Generated if a Custom Script SSO Agent is configured in Inventory. FortiNAC sends user ID and IP address as parameters to the script each time a host connects to the network. Event indicates that the script configured in the Inventory failed to run.
Conference Created	Using guest/contractor accounts you can create a batch of conference user accounts. This event is generated when those accounts are created and indicates the number of accounts created.
Contact Established	Contact with a device has been established.
Contact Lost	Contact with a device has been lost.
Container Created	New container has been created in the database. Containers are a grouping mechanism for devices that display in the Inventory.
Container Destroyed	Container has been deleted from the database. Deleting a container deletes all of the devices it contains.
Database Archive/Purge Failure Database Archive/Purge Success	Indicates whether or not the scheduled database archive/purge was successful.
Data Export Completed	Shows the date and who exported, and the number of records from the Event Management page. The data types that can be exported are User Accounts, Adapter, Device Profiling Rules, etc.
Database Backup Failure Database Backup Success	Indicates whether or not the scheduled database backup was successful.
Database Replication Error	Occurs in a high availability situation when the MasterLoader database is not replicating. Can also be triggered when the database on the secondary server is not running.
Database Replication Succeeded	Occurs in a high availability situation when the MasterLoader database is successfully replicated to the secondary server.
De-authenticated	User logged off from host.

Event	Definition
De-authentication Failure	Unable to log off user from host. User not found.
Deleted Host Successfully	Host or FortiNAC user has been successfully deleted from the database. If multiple records are deleted at once, a separate event is generated for each record.
Device Cold Start	Device was restarted using the power switch.
Device Created	New managed device has been created in the database.
Device Destroyed	Managed device has been deleted from the database.
Device Fingerprint Changed	Host is using a different operating system than the one with which the host was registered. This could occur on a host with a dual-boot. For example, the host registers with a Windows operating system. The user later boots the host using Linux and tries to access the network. That change would trigger this event. An upgrade within a family of operating systems would not normally trigger this event, such as from Windows XP to Windows Vista. Operating system is determined by the DHCP fingerprint.
Device Identity	No longer used.
Device Link	A device has linked to port X on the network.
Device Link Down	A device link goes down on a specific port because a device was disconnected from the port.
Device Link Up	Generated when a device link goes up on a specific port.
Device Profile Rule Match	A rogue host has matched a Device Profiling rule allowing it to be assigned a device type and registered.
Device Profiling Automatic Registration	A rogue host has been registered by device profiling based on a device profiling rule.
Device Profiling Rule Missing Data	Indicates that device profiler cannot compare a rogue against a rule because FortiNAC does not have enough information about the rogue, such as a DHCP fingerprint. If device profiler cannot compare a rogue against a rule it does not continue processing that rogue, and moves on to the next rogue.
Device Rule Confirmation Failure Device Rule Confirmation Success	Devices identified by a Device Profiling rule maintain their association with that rule. If enabled, the associated rule and the device are checked periodically to see if the rule is still valid for the device. These event messages indicate whether or not the device matched the associated rule.
Device Warm Start	Device was restarted from the command line interface.
DHCP Host Name Changed	Generated when a known host connects to the network and its hostname is different. Indicates that the hostname in the database associated with the MAC address and existing DHCP finger print for that host is different.

Event	Definition
Directory Connection Failure	The connection to a directory, such as Active Directory or LDAP, failed. The directory could have refused the connection because the user name and password were incorrect. This event can be triggered when testing the connection to the directory with Test on the Directory Configuration window.
Directory Group Disabled Directory Group Enabled	Users can be disabled/enabled in a directory, such as LDAP, based on group membership. When the FortiNAC database synchronizes with the directory, users that are members of the group are enabled. Users that are not members of the group are disabled.
Directory Synchronization Failure Directory Synchronization Success	Indicates whether or not a directory, such as Active Directory or LDAP, synchronized with the user database. Could be caused if FortiNAC fails to connect to the directory. This synchronization is a one time task done when the directory is configured. See Schedule synchronization on page 879 .
Directory User Disabled Directory User Enabled	Users can be disabled/enabled in a directory, such as LDAP. When the FortiNAC database synchronizes with the directory, users can be disabled/enabled based on their directory setting.
Disable Host Failure Disable Host Success	Generated when a user manually disables a host on the Host View. Indicates whether or not the host was successfully disabled.
Disable Hosts Failure Disable Hosts Success	Indicates whether or not hosts in a group were successfully disabled using a scheduled task.
Disable Port Failure Disable Port Success	Indicates whether or not a particular port was disabled by an alarm action.
Disable Ports Failure Disable Ports Success	Indicates whether or not ports in a particular group were disabled by a scheduled task.
Disable User Success	Indicates that a user selected from the user view was successfully disabled.
Disabled Authenticated	No longer used.
Disassociate	Host Disassociated
Discovery Completed	The device discovery process that adds new devices to FortiNAC has completed. IP address range is included in the completion message.
Duplicate Host For Device	No longer used.
Duplicate Physical Address	No longer used.
Duplicate Users Found in Directory	Two users with the same last name and/or ID were found in the directory. FortiNAC is case in-sensitive. For example, two users with last names listed as SMITH and smith are treated as if they were the same person. The newer of the two users is ignored.
Email Failure	Alarms can be configured to send E-mail Notifications to FortiNAC administrative users. If the administrative user has no e-mail address or the e-mail fails in any other way, this event is generated.

Event	Definition
Enable Host Failure Enable Host Success	Indicates whether or not a host selected from the Host View was successfully enabled.
Enable Hosts Failure Enable Hosts Success	Indicates whether or not hosts in a group were successfully enabled using a scheduled task.
Enable Port Failure Enable Port Success	Indicates whether or not a particular port has been enabled by an alarm action in response to a previous event.
Enable Ports Failure Enable Ports Success	Indicates whether or not ports in a particular group were enabled by a scheduled task.
Enable User Success	Indicates that a user selected from the user view was successfully enabled.
Endpoint Compliance Configuration Modified	Generated whenever an endpoint compliance configuration is modified.
Endpoint Compliance Configuration Platform Setting Modified	Generated whenever an endpoint compliance configuration platform setting is modified.
Endpoint Compliance Modified	Generated whenever an endpoint compliance is modified.
Enterasys Dragon Violation	Enterasys Dragon is an Intrusion Protection/Detection System. An event is generated when an intruder is detected.
Entitlement Polling Failure	(Requires version 8.8.10, 9.1.4, 9.2.0 or above) Generated when there is an error communicating or processing license entitlements data from Forticloud over TCP 443. Entitlement polling is required for Subscription Licenses. Refer to the Deployment Guide in the Document Library for Open Port requirements.
Entitlement Polling Success	(Requires version 8.8.10, 9.1.4, 9.2.0 or above) Generated when communication and processing of license entitlements data from Forticloud successfully completes.
Failed to Disable Adapters	Attempted to disable hosts using an Alarm Action. Hosts failed to be disabled.
Failed to Disable HP Port Security	Scheduled task that enables port security configuration on all HP/NT devices in an associated group has failed.
Failed to Enable Adapters	Attempted to enable hosts using an Alarm Action. Hosts failed to be enabled.
Failed to Enable HP Port Security	Scheduled task that enables port security configuration on all HP/NT devices in an associated group has failed.
FireEye IPS High Violation	Generated whenever a high violation event is received from FireEye.
FireEye IPS Low Violation	Generated whenever a low violation event is received from FireEye.
FireEye IPS Medium Violation	Generated whenever a medium violation event is received from FireEye.
Firewall Session Poll Failed Firewall Session Poll Succeeded	For details see Firewall session polling.
FORTIGATE-6.0_HIGH_SEVERITY	FortiNAC received a FortiGate security alert. Fort details see Security Incidents.

Event	Definition
FORTIGATE-6.0_LOW_SEVERITY FORTIGATE-6.0_MEDIUM_SEVERITY	
FortiOS 4.0 High Violation	Generated whenever a high violation event is received from FortiOS 4.0.
FortiOS 4.0 Low Violation	Generated whenever a low violation event is received from FortiOS 4.0.
FortiOS 4.0 Medium Violation	Generated whenever a medium violation event is received from FortiOS 4.0.
FortiOS 5.0 High Violation	Generated whenever a high violation event is received from FortiOS 5.0.
FortiOS 5.0 Low Violation	Generated whenever a low violation event is received from FortiOS 5.0.
FortiOS 5.0 Medium Violation	Generated whenever a medium violation event is received from FortiOS 5.0.
Found Ignored MAC address	A host or device has connected with a MAC address that is in the MAC address Exclusions list. This connection is not being managed by FortiNAC and the host or device has access to the production network. See MAC address exclusion on page 1009 .
Found Microsoft LLTD or Multicast Address	A host or device has connected with a MAC address in the Microsoft LLTD or Multicast Address range. Those ranges are managed in the MAC address Exclusion list. FortiNAC ignores these MAC addressed for 48 hours after the first one is seen and then treats them as rogues unless the configuration is updated on the MAC address Exclusion list. See MAC address exclusion on page 1009 .
Gaming Device Registration	A gaming device was registered by a user.
Generate/Revoke Certificates via REST API	For details see section Certificate in the REST API reference manual. https://docs.fortinet.com/document/fortinac-f/7.4.0/rest-api/309424/certificate
Group Does Not Exist for Scan	FortiNAC attempted to perform a scan or scheduled task for a particular group and the group no longer exists in the database. Either recreate the group or remove the scan or scheduled task.
Guest Account Created	New guest account is created.
Guest Account Deleted	Guest account is deleted.
Guest/Contractor Pre-allocation Critical	No longer used. If you are setting up Guest/Contractor users in advance, an event can be generated if you set up more Guest/Contractor users than you have licenses.
Guest/Contractor Pre-allocation Warning	No longer used. If you are setting up Guest/Contractor users in advance, an event can be generated if you set up enough Guest/Contractor users to use 75% of the available licenses.

Event	Definition
Hard Disk Usage Critical	Generated when the disk usage critical threshold is reached. This threshold is a percentage of the space allocated for the bsc and var partitions. The percentage is calculated for each partition separately. When any one partition reaches the threshold the event is generated. Thresholds calculated for individual partitions are never combined. Therefore if the combined total crosses the threshold, no event is generated. Default = 95%
Hard Disk Usage Warning	Generated when the disk usage warning threshold is reached. This threshold is a percentage of the space allocated for the bsc and var partitions. The percentage is calculated for each partition separately. When any one partition reaches the threshold the event is generated. Thresholds calculated for individual partitions are never combined. Therefore if the combined total crosses the threshold, no event is generated. Default = 85%
Host Aged Out	Host has been removed from the database based on the time or expiration date on the associated Host Properties window. See Properties on page 221 .
Host Application Violation	Generated against a FortiNAC host based on the IP, MAC, or ID information contained within an Application Violation trap. If IP, MAC address, or user ID match any records in the FortiNAC database, this event is generated. See Application Violation in this list.
Host Application Violation Reset	Generated against a FortiNAC host based on the IP, MAC, or user ID information contained within an Application Violation Reset trap. If IP, MAC address, or user ID match any records in the FortiNAC database, an event is generated. The reset event occurs when the host is no longer in violation. See Application Violation in this list.
Host At Risk	An administrative user marked a selected host At Risk or the host failed a scan.
Host At Risk Failure Host At Risk Success	Indicates whether an alarm action triggered by an At Risk host succeeded or failed.
Host At Risk Status Not Enforced	Generated whenever a host fails a scan, but it is not enforced.
Host CLI Task Success Host CLI Task Failure	Indicates whether or not the CLI commands associated with host/adaptor based ACLs have been successful.
Host Connected	Generated whenever a registered host connects to the network.
Host Copied From NCS	In an environment where multiple FortiNAC appliances are managed by a FortiNAC Manager, hosts and their corresponding information can be copied from one appliance to another based on settings in the FortiNAC Manager under System > Settings > Network Control Manager > Server Synchronization . When hosts are copied from one appliance to another this event is generated.
Host Created	Generated whenever a host is created.
Host Destroyed	Generated whenever a host is destroyed.
Host Disassociated	Generated whenever a host is destroyed.

Event	Definition
Host Disconnected	Generated whenever a registered host disconnects from the network.
Host Identity Changed	Indicates that a registered host's name or operating system has changed since the last time it was read by the Persistent Agent or Dissolvable Agent, and that it is possibly a dual boot device. This could also indicate MAC spoofing. An operating system change , such as an upgrade could also trigger this event.
Host Pending At Risk	A host failed a scan for an endpoint compliance policy. The policy was configured for delayed remediation indicating that hosts that fail the scan are not sent to remediation for x number of days. The event is generated when the host is marked Pending At Risk. Scan status "Failure Pending" triggers this event.
Host Registration Failure Host Registration Success	Host has gone to the Registration page and the user attempted to register the host. Indicates whether the registration succeeded or failed.
Host Rejected - No MAC	Host rejected because it is missing a MAC address.
Host Rejected - No VLAN	Host rejected because there is no VLAN defined for current state.
Host Safe	Generated when a user goes to System > Settings > Control > Quarantine . On the Quarantine view there is a button that allows the user to mark all hosts as Safe. If this button is clicked the event is generated for each host that was affected.
Host Safe Failure Host Safe Success	Indicates whether or not an alarm action associated with marking a host as safe has failed. See Host Safe on page 759 in this list.
Host Session Logged On Host Session Logged Off	Agent has detected that the user has logged on or off the host. Applies only to Windows hosts.
Host Session changed Remote Control status	A Windows Session for an Active Directory user has changed remote control status. It is either now remotely controlled or no longer remotely controlled
Host Session Connected to Console	A Windows Session for an Active Directory user connected to the Console.Event is generated on the Adapter
Host Session Disconnected from Console	A Windows Session for an Active Directory user was disconnected from the Console.Event is generated on the Adapter
Host Session Locked	A Session for an Active Directory user was locked. The session is still active and this is not equivalent to a logout.Event is generated on the Adapter
Host Session Remotely Connected	Connected to remote desktop
Host Session Remotely Disconnected	Disconnected from remote desktop
Host Session Unlocked	A Session for an Active Directory user was unlocked. The session is still active and this is not equivalent to a login.Event is generated on the Adapter
Incomplete User Found in Directory	FortiNAC requires the Last name and ID fields for each user. If either of those fields is missing, the user record is incomplete.

Event	Definition
Interface Status Failure Interface Status Success	Indicates whether or not the Update interface status scheduled task was successful. The task reads and updates the interface status for each port on the devices in the associated groups.
Internal Scheduled Task Failure Internal Scheduled Task Success	Indicates whether or not a scheduled task has failed. The name of the task is provided.
Invalid Physical Address	The MAC address of the specified host or device is not recognized by FortiNAC because the corresponding vendor OUI is not in the FortiNAC database. Update the vendor OUI database either manually or by using Auto-Def Updates. See article Verifying Vendor OUIs .
L2 Poll Failed L2 Poll Succeeded	Indicates whether or not FortiNAC successfully contacted the device to read the list of connected hosts.
L3 Poll Failed L3 Poll Succeeded	Indicates whether FortiNAC successfully read IP address mappings from a device.
Load In Limit Exceeded	No longer used. Max % In setting on the Bandwidth window has been met or exceeded.
Load In Limit Rearmed	No longer used. After the first "Load In Limit Exceeded" event occurs the server does not generate a "Load In Limit Rearmed" event until the percentage of bandwidth bytes in falls below Rearm % In value.
Load Out Limit Exceeded	No longer used. Max % Out setting on the Bandwidth window has been met or exceeded.
Load Out Limit Rearmed	No longer used. After a "Load Out Limit Exceeded" event occurs the server creates a "Load Out Limit Rearmed" event once the percentage of bytes out falls below this the Rearm % Out value.
Local Host Session changed Remote Control status	A Windows Session for a Local user has changed remote control status. It is either now remotely controlled or no longer remotely controlled
Local Host Session Connected to Console	A Session for a Local user connected to the Console.Event is generated on the Adapter.
Local Host Session Disconnected from Console	A Session for a Local user was disconnected from the Console.Event is generated on the Adapter.
Local Host Session Remotely Connected	A Remote Windows Session connected.
Local Host Session Remotely Disconnected	A Remote Windows Session disconnected.
Local Host Session Unlocked	A Session for a Local User was unlocked.

Event	Definition
Lost Contact with Persistent Agent	This event can only be generated accurately when FortiNAC has up-to-date network connectivity data (in order to determine a host's online status). This requires the following: - Wired network devices are being polled at a regular interval (typically 1 hour). - Wired network devices are sending either Link Up/Link Down or Mac Notification traps. - Wireless devices are being polled at a regular interval (typically 15 minutes).
MAC change event on uplink	This event is generated when a MAC notification trap is received for a port in FortiNAC is any of the uplink types.
MAC Learned	Generated when MAC Notification "MAC Add" or "MAC Move" syslog messages/SNMP traps are received from supported devices. Occurs when the switch has added to its forwarding table the MAC address of a connecting host. Note: Not generated for infrastructure devices (such as Access Points).
MAC Removed	Generated when MAC Notification "MAC Delete" or "MAC Move" syslog messages/SNMP traps are received from supported devices. Occurs when the switch has removed the MAC address of a host that has disconnected. Note: Not generated for infrastructure devices (such as Access Points).
Management Established	Generated when management of a device is established.
Management Lost	Generated when management of a device is lost.
Map IP to MAC Failure	No longer used.
Map IP to MAC Success	Mapping IP addresses to physical addresses for a selected group using a scheduled task failed or succeeded.
Maximum Blacklist Clear Attempts Reached	Generated when the maximum number of attempts to remove a MAC address from a device's black list has been exceeded. Currently the maximum is set to 3 attempts.
Maximum Blacklist Clear Attempts Reached	Maximum number of attempts to remove a host from a controller's blacklist have been reached and the host remains on the blacklist.
Maximum Concurrent Connections Critical	Concurrent connection licenses in use has reached or exceeded 95% of total licenses. Threshold is configurable. See Event thresholds on page 774 .
Maximum Concurrent Connections Exceeded	Concurrent connection licenses in use has reached 100% of total licenses.
Maximum Concurrent Connections Warning	Concurrent connection licenses in use has reached or exceeded 75% of total licenses. Threshold is configurable. See Event thresholds on page 774 .
Maximum Concurrent Physical Address Warning	No longer used. Generated when host connections exceed 6000 or 12000 depending on the size of the appliance.
Maximum Guest/Contractor Critical	No longer used. Guest manager licenses in use has reached or exceeded 95% of total licenses. Threshold is configurable.

Event	Definition
Maximum Guest/Contractor Exceeded	No longer used. Guest manager licenses in use has reached 100% of total licenses.
Maximum Guest/Contractor Warning	No longer used. Guest manager licenses in use has reached or exceeded 75% of total licenses. Threshold is configurable.
Maximum Host Warning	No longer used. Access Manager licenses in use has reached or exceeded 75% of total anesthesiologist is configurable.
Maximum Hosts Critical	No longer used. Access Manager licenses in use has reached or exceeded 95% of total licenses. Threshold is configurable.
Maximum Hosts Exceeded	No longer used. Access Manager licenses in use has reached 100% of total licenses. No new accounts can be created.
Maximum Known Device Critical	No longer used. Device Tracker licenses in use has reached or exceeded 95% of total licenses. Threshold is configurable.
Maximum Known Device Warning	No longer used. Device Tracker licenses in use has reached or exceeded 75% of total licenses. Threshold is configurable.
Maximum Known Devices Exceeded	No longer used. Device Tracker licenses in use has reached 100% of total licenses.
Maximum User Critical	No longer used. Shared Access Tracker licenses in use has reached or exceeded 95% of total licenses. Threshold is configurable.
Maximum User Warning	No longer used. Shared Access Tracker licenses in use has reached or exceeded 75% of total licenses. Threshold is configurable.
Maximum Users Exceeded	No longer used. Shared Access Tracker licenses in use has reached 100% of total licenses.
MDM Host Compliance Failed	Host failed MDM scan
MDM Host Compliance Passed	Host passes MDM scan
MDM Host Created	Host was added to the database from MDM import
MDM Host Destroyed	Host is deleted from the database because it is no longer found on a poll of the MDM. This can occur if the corresponding record in the MDM database was either removed or disabled. "Remove Hosts Deleted from MDM Server" option in MDM services must be enabled.

Event	Definition
MDM Poll Failure	MDM poll did not complete
MDM Poll Success	MDM poll completed
Memory Usage Critical	Generated when the memory usage critical threshold is reached for the appliance. This threshold is a percentage of the total allocated memory. Default = 95% Threshold is configurable. See Event thresholds on page 774 .
Memory Usage Warning	Generated when the memory usage warning threshold is reached for the appliance. This threshold is a percentage of the total allocated memory. Default = 85% Threshold is configurable. See Event thresholds on page 774 .
Message	Cabletron/Enterasys Event Log Message OID = 1.3.6.1.4.1.52.1280
Multi-Access Point Detected	Generated when multiple MAC addresses are detected on a port. Requires "Enable Multi-Access Detection" option to be selected. See Network device on page 910 . Note: This event does not generate for ports in the Authorized Access Points group.
Multihomed Host Detected Multihomed Host Fixed	Triggers when Detect Multihoming is enabled in scan and host has multiple adapters connected to the network. See Create or edit a configuration . See also KB article https://community.fortinet.com/t5/FortiNAC/Technical-Tip-SSID-AP-check-and-Multihome-detection-with/ta-p/282330
NAT Device Registered	Generated when a NAT Device (router) is registered.
Nitro Security Violation Nitro Threat Level 1 - 6	Generated based on traps received from the NitroGuard Intrusion Protection/Detection system on your network. The IPS/IDS must be modeled in your Inventory.
No CDP Announcement	Generated when a device that has sent at least one CDP announcement has stopped sending those announcements. This is based on the polling time set for the device. For example if the poll time is one hour, a new event message is sent each time the hour elapses with no message from the device.
Operating System Is Up to Date	Indicates that there are no new updates available after the operating system update status task is run (1pm every Sunday, by default).
Operating System Status Check Failure	Indicates that the operating system update check failed due to multiple running checks. This may be caused by a configuration or network issue.
Operating System Update Initiated	Indicates that an operating system update was started from the admin UI. See Description on page 1 .
Operating System Updates Available	Indicates that there are updates available after the operating system update status task is run (1pm every Sunday, by default).
Packeteer Configuration Failure Packeteer Configuration Success	No longer used. Indicates whether or not communication has been established with the Packeteer PacketShaper software after Packeteer has been modeled in the Inventory.

Event	Definition
Packeteer Monitor	If Packet Shaper has been configured to generate threshold violation events and if a threshold violation occurs, the event triggers an SNMP trap from PacketShaper to FortiNAC. This trap causes FortiNAC to generate a Packeteer Monitor event.
Packeteer Monitor 2	No longer used. If a Packeteer product has been configured to generate events for OID 13.6.1.3.6.1.4.1.2334.1.1 and the event triggers an SNMP trap from the Packeteer to FortiNAC. This trap causes FortiNAC to generate a Packeteer Monitor 2 event.
PaloAlto Firewall High Violation PaloAlto Firewall Low Violation PaloAlto Firewall Medium Violation	FortiNAC received a violation syslog message from Palo Alto (High Violation, Medium Violation or Low Violation). See Palo Alto Networks Integration https://docs.fortinet.com/document/fortinac-f/7.2.0/palo-alto-networks-integration/341880/syslog-management#/document/fortinac-f/7.2.0/palo-alto-networks-integration/341880/syslog-management#_Toc130369411
PatchLink Compliant PatchLink Non Compliant	Indicates whether or not Patchlink detected endpoint within compliance. For details see Patch management. https://docs.fortinet.com/document/fortinac-f/7.4.0/administration-guide/420671/patch-management
Persistent Agent Communication Resumed	Persistent Agent Contact Status has been restored to normal. This event is only generated on hosts running Persistent Agent 4.0 or better.
Persistent Agent Not Communicating	This event can only be generated accurately agents when FortiNAC has up-to-date network connectivity data (in order to determine a host's online status). This requires the following: - Wired network devices are being polled at a regular interval (typically 1 hour). - Wired network devices are sending either Link Up/Link Down or Mac Notification traps. - Wireless devices are being polled at a regular interval (typically 15 minutes).  This event is only generated on hosts running Persistent Agent 4.0 or better.
Persistent Agent Scan Not Performed	This event can only be generated accurately when FortiNAC has up-to-date network connectivity data (in order to determine a host's online status). This requires the following: - Wired network devices are being polled at a regular interval (typically 1 hour). - Wired network devices are sending either Link Up/Link Down or Mac Notification traps. - Wireless devices are being polled at a regular interval (typically 15 minutes).
Policy Warning	Host was scanned by an endpoint compliance policy. The host does not meet all of the scan requirements, but the scan rules state that a warning be issued instead of making compliance a requirement. Scan status "Warning" triggers this event.

Event	Definition
Poll For Hosts Failure Poll For Hosts Success	No longer used. Indicates whether a scheduled task to poll switches for hosts has succeeded or failed. Switches are contained in a device group and that group is polled.
Port CLI Task Failure Port CLI Task Success	Indicates whether a CLI configuration applied to a port ran and failed or succeeded.
Port(s) Added To Group	Shows the person who added, and the name of the new port added to the group.
Port(s) Removed From Group	Shows the person who removed, and the name of the port removed from the group.
Port in Authorized Access Points Group	Scheduled task for a port in the Authorized Access Points group failed.
Port in Authorized Access Points Group	Failed to enable/disable port because it is in the Authorized Access Points group.
Port Link Down Port Link Up	Trap received from the switch each time there is a link up or a link down on a port. Link up and link down happen each time a host is switched from one VLAN to another.
Port Security Incomplete	Maximum number of users on a port has been reached.
Port Segmented	Trap received from an Enterasys or Cabletron switch indicating that a link is down. This port may have been logically disconnected due to an excessive collision level or it may be physically disconnected.
Port Uplink Configuration Modified	An administrator modified the uplink setting of a port. The switch name, port and administrator are included in the event.
Possible MAC address Spoof	Indicates that the same MAC address has been detected on two different devices simultaneously. One is possibly spoofing the other's MAC address. This event is generated based upon the value of the MAC Spoof Time Delay configured under System > Settings > Network device . See Network device on page 910 for details. Note: FortiNAC cannot distinguish which port has the legitimate host connected. Therefore, if the event is mapped to an alarm, the alarm action (such as disabling the port) will apply to both ports triggering the event.
Possible NAT Device, MAC Spoofed	This event has been replaced with NAT Device Registered. It remains visible to allow you to restore an old backup and view occurrences of this event. See NAT Device Registered on page 763 in this list.
Possible NAT User	Generated on each host. One per MAC address on the NATd host. For example, if a host has both a wired and wireless connection, an event is generated for each.
Process Memory Usage Critical	Generated when the memory usage critical threshold is reached for the process. This threshold is a percentage of the total allocated memory. Default = 95%
Process Memory Usage Warning	Generated when the memory usage warning threshold is reached for the process. This threshold is a percentage of the total allocated memory. Default = 85%

Event	Definition
Process Thread Count Critical	Generated when the process thread count warning threshold is reached. This threshold is a specific number of threads the process is using. Default = 575 This event is disabled by default. The threshold will dynamically increase by 25 for every 8 CPU cores that are added.
Process Thread Count Warning	Generated when the process thread count warning threshold is reached. This threshold is a specific number of threads the process is using. Default = 500 This event is disabled by default. The threshold will dynamically increase by 25 for every 8 CPU cores that are added.
Profile Modified	Generated when a user modifies a user/host profile. Event message contains user information for the user who made the change, whether the change was an add, remove or replace, and the complete profile after the changes.
RADIUS Rate Exceeded	Generated when the 60 requests-per-second threshold is exceeded. This event is disabled by default.
RADIUS Time Threshold	Indicates that the time threshold for a response from the RADIUS server has been exceeded. This threshold is not configurable.
Regained Contact with Persistent Agent	Host has regained contact with the Persistent Agent .
Remote Access Excessive Session Process Time	Generated when the time to process the remote client exceeds a threshold (set through the "MaxClearTime" attribute on the ASA device).
Reports Purged	Lists the file names of all reports that were deleted when reports were purged from the /home/cm/reports directory.
REST API Failure	Error when FortiNAC tries to communicate with the device using REST API.
Scan Does Not Exist For Scheduler Task	FortiNAC has attempted to run a scan using a scheduled task. The scan referred to in the task no longer exists in the database. You must either recreate the scan or remove the scheduled task from the scheduler.
Secondary Contact Lost	Event triggered when the primary loses contact with the secondary.
Security Risk Host	Event triggered when a host is marked at risk due to an agent scan failure. Associated events are "Host Passed Security Test" and "Host Security Test - Delayed Failure."
Service Down - Analytics Agent	Event triggered when the service is down and it is required for FortiNAC to send data to Analytics.
Service Down - Radius Service Down - Samba Service Down - Winbind	Event triggered when one of the listed the services is no longer running and it is required for the RADIUS Manager.

Event	Definition
Service Down - Tomcat Admin Service Down - Tomcat Portal Service Down -dhcpd Service Down -httpd Service Down -mysqld Service Down -named Service Down -sshd	Event triggered when a specific service is no longer running. These services are required. FortiNAC tries to restart the service every 30 seconds. In a high availability environment, failover occurs after the fourth failed restart attempt. For the httpd service: After the system confirms that the httpd service is running, the system also attempts to connect to ports 80 and 443. If the system fails to connect to either port, the httpd service is restarted. If the primary is unable to communicate with the secondary to confirm it is running, service down will not trigger a failover.
Service Started - Analytics Agent	Event triggered when the service is started. This service is required and must be running in order to use Analytics.
Service Started - Tomcat Admin Service Started - Tomcat Portal Service Started -dhcpd Service Started -httpd Service Started -mysqld Service Started -named Service Started -sshd	Event triggered when one of the listed services is started. These services are required and must be running in order to use FortiNAC.
Service Started -Radius Service Started - Samba Service Started - Winbind	Event triggered when one of the listed services is started. These services are required in order to use RADIUS Manager.
Set Default VLAN Failure Set Default VLAN Success	When a host disconnects from a port, the port can be set to return to its default VLAN. Indicates whether or not the port successfully returns to the default VLAN.
SNMP Failure	Generated when FortiNAC receives an SNMP failure during communication with a SNMP enabled Network Device. This includes any error message received from the SNMP packet.
SNMP Read Error	Did not receive all data when reading a switch using SNMP. Device name and error code are included in the event message.
Sophos AntiVirus: Virus Found	Sophos AntiVirus can be configured to send traps to FortiNAC when a virus is found on a host. Host information is included in the trap. If a Sophos Trap is received, this event is generated.
Sourcefire Error Sourcefire IPS Action Sourcefire IPS High Violation Sourcefire IPS Low Violation Sourcefire IPS Medium Violation	Generated based on syslog events received from an Intrusion Protection/Detection system on your network. The IPS/IDS must be modeled in your Inventory. Sourcefire IPS Action: Indicates that an action has been triggered by a syslog message from Sourcefire.
StealthWatch	SNMP trap has been sent from a StealthWatch device OID = 1.3.6.1.4.1.8712
StealthWatch Email Rejects	Host is receiving a significant number of rejected mail attempts.

Event	Definition
StealthWatch Email Relay	Host is operating as an email relay.
StealthWatch High Concern	A host has exceeded the Concern Index threshold set for it. This usually means that an inside host is no longer operating as it was during the tuning period and should be examined for possible compromise, misuse, or policy violations. An external host with a High Concern index is often attempting to violate your network integrity.
StealthWatch High File Sharing	Host is transferring files.
StealthWatch High Volume Email	Host is infected with an email worm.
StealthWatch Max Flows Initiated	Host has had an excessive number of total flows active.
StealthWatch New Flows	Indicates that a host exceeds a total number of new flows in a 5-minute period.
StealthWatch Port Flood	The host has attempted to connect on an excessive number of ports on the Target IP. This may indicate a DoS attack or an aggressive scan by the source IP.
StealthWatch Suspect Long Flow	Host has a long duration flow.
StealthWatch SYN Flood	The host has sent an excessive number of TCP connection requests (SYN packets) in a 5-minute period. This may indicate a DoS attack or non-stealthy scanning activity
StealthWatch Worm Activity	A host has scanned and connected on a particular port across more than one subnet. The details section of this alarm specifies the port on which the activity was observed.
StealthWatch Worm Propagation	Host has scanned and connected on port 5 across more than 1 subnet.
StealthWatch Zone Violations	Host has connected to a server in a zone that it is not allowed to access.
StoneGate IPS High Violation StoneGate IPS Low Violation StoneGate IPS Medium Violation	Generated based on syslog events received from an Intrusion Protection/Detection system on your network. The IPS/IDS must be modeled in your Inventory. See Syslog files on page 963 .
StoneGate Violation	Generated based on syslog events received from an Intrusion Protection/Detection system on your network. The IPS/IDS must be modeled in your Inventory. See Syslog files on page 963 .
Success Disabling Port Security Success Enabling Port Security	Generated when the Enable or Disable HP/NT Port Security scheduled task runs successfully. This task enables or disables port security configuration on all HP/NT devices in the selected group. Port Security is used to disable hosts if DeadEnd VLANs are not used on the network.
Sync Initiated	(FortiNAC versions 9.1.3 and above) Generated when a synchronization of servers by Control Manager has been triggered. Provides server IP, the user who triggered the sync and status.

Event	Definition
Synchronize Users with Directory Failure Synchronize Users with Directory Success	Indicates whether or not the FortiNAC user database has successfully synchronized with the selected directory such as LDAP or Active Directory. These events are triggered by the failure or success of the scheduled synchronization set up on the Directory Configuration window. See Configuration on page 870 .
Syslog Error	Generated when the FortiNAC server receives an inbound syslog message for a host that is not currently managed by FortiNAC.
System Automatically Restarted	Server was restarted because a primary system process was down. Processes include: MasterLoader, IP to MAC, Communication and Nessus. This event was System Restart in prior versions.
System Backup Failure System Backup Success	Indicates whether a system backup has succeeded. The system backup is run by a scheduled task. The system backup may succeed, but will still fail if remote backup is enabled and fails. It is recommended that you create an alarm action to send an email if system backup fails.
System Created Uplink	If Uplink Mode on a Port's properties is set to Dynamic, FortiNAC converts the port to an uplink port when the number of MAC addresses on the port exceeds the System Defined Uplink count and generates this event.
System Fail Over	In a high availability environment, this event indicates that the primary server has failed and the secondary has taken over.
System Power Off	Indicates that the user specified in the event message powered off the FortiNAC server. See Power management on page 986
System Reboot	Indicates that the user specified in the event message rebooted the FortiNAC server. See Power management on page 986 .
Temporary exception for port ** has been successfully set, un-enforcement is between ** and **.	Generated when Temporary Port Exception is configured.
Temporary exception for the port ** has been completed and enforcement begins for the port.	Generated after configured Temporary Port Exception expires.
Temporary exception for port ** has been successfully cancelled.	Generated when configured Temporary Port Exception is cancelled.
TippingPoint SMS High Violation TippingPoint SMS Low Violation TippingPoint SMS Medium Violation	Generated based on syslog events received from an Intrusion Protection/Detection system on your network. The IPS/IDS must be modeled in your Inventory. See Syslog files on page 963 .
Top Layer IPS High Violation Top Layer IPS Low Violation Top Layer IPS Medium Violation	Generated based on syslog events received from an Intrusion Protection/Detection system on your network. The IPS/IDS must be modeled in your Inventory. See Syslog files on page 963 .

Event	Definition
Unauthorized SSID/VLAN	No longer used.
Unknown User in Group	No longer used.
Unsupported Trap	Generated when FortiNAC receives a trap that it cannot interpret from a device. The device's OID is included in the event.
Update SSID Failure Update SSID Success	SSID assignment scheduled task maps VLAN IDs to SSIDs. Event indicates whether or not the task succeeded.
Update VLAN ID Failure Update VLAN ID Success	Indicates that the user specified in the event message powered off the FortiNAC server. See Power management on page 986 . Update Default VLAN Values scheduled task sets the Default VLAN value for the port in FortiNAC device model to the value entered in the scheduled task. Event indicates whether or not the task succeeded.
User Connected to Host Console	A user connected to the console. Event is generated on the User
User De-authenticated on Adapter	The same event as De-authenticated but generated on the Adapter
User Disconnected from Host Console	A Windows Session for an Active Directory user connected to the Console. Event is generated on the User
User Locked Session	A Session for an Active Directory user was locked. The session is still active and this is not equivalent to a logout. Event is generated on the User
User Remotely Connected to Host	A Remote Windows Session connected to a Host. Event is generated on the User
User Remotely Disconnected from Host	A Remote Windows Session disconnected from a Host. Event is generated on the User
User Session changed Remote Control status	A Windows Session for a Local user has changed remote control status. It is either now remotely controlled or no longer remotely controlled. Event is generated on the User.
User Unlocked Session	A Session for an Active Directory user was unlocked. The session is still active and this is not equivalent to a login. Event is generated on the User
User Cancelled VLAN Switch	(FortiNAC version F 7.6.5 +) User selected "cancel" to Persistent Agent popup acknowledgment for VLAN to transition from a remediation VLAN. An Event-to-Alarm Mapping can be enabled to prevent the VLAN change. Requires Persistent Agent F 7.6.2 +. Alarm Mapping Example: Severity: Informational Trigger Event: User Cancel VLAN Switch Acknowledgement Trigger Rule: One Event to one Alarm Action: Host Security Action Primary Task: At Risk - VLAN Switch Canceled Run Secondary Task (Enabled)

Event	Definition
	- After: 60 mins <-- After 60 minutes, the host will be marked Safe and VLAN switched back to production network. If the secondary task is not configured, host remains in remediation VLAN until user selects OK when prompted to change VLAN.

Event management

Event management allows you to specify which events to generate and whether to log the event records on another server in addition to the local appliance. You can limit the number of events generated by selecting a group for each event. Event messages are only created when the event occurs within the specified group.

Specify threshold values for the self-monitoring events by clicking **Event Thresholds**. These thresholds affect the **Performance Summary Panel** on the dashboard. They can be edited here or from the **Performance Summary Panel**. See [System Performance on page 94](#) for additional information.

Some events are generated frequently and may not be necessary for day to day operations. Review the list of events and determine which ones to enable to provide you with the most useful feedback. You may choose to enable an event for a short period of time, such as to find a particular host when it connects to the network. See the example below for a scenario in which enabling a particular event might be useful.

Example: Finding a stolen device

This is a scenario for locating a stolen or missing host:

1. Create a group that contains only the information for that host (including all wired and wireless sibling records).
2. Enable the host connected event for the new group. When the stolen host connects to the network through the wired or wireless connection, a host connected event is generated.
3. Map the host connected event to an alarm to receive a notification that the host has connected. You may also take an action against that host if you specified one in the mapping.
4. When you are notified that the stolen host has connected to the network, use the Host View to determine the device and port to which this host is connected.

Events are generated for all components, such as devices, hosts or ports, unless you reduce the output by selecting a specific group. See [Events and alarms list on page 750](#) for event definitions.

Events can be sent to an external log host. See [Log events to an external log host on page 776](#).

Settings

Fields used in filters are also defined in this table.

Field	Definition
Event Thresholds	Opens the Event Thresholds dialog to set thresholds to monitor license usage, memory usage, process thread counts, and disk space. Exceeding these thresholds generates specific events. See Event thresholds on page 774 .
Events	
Log	Indicates the state of the selected event and where it will be logged if it is generated. • Disabled: Event is disabled and will not be generated or logged anywhere. • Internal: Logs only to an internal events database. • External: Logs only to an external host. (Note: This option assigns events a database ID value of "-1" which may not be accepted by some external log servers). • Internal & External: Logs both to an internal events database and an external host.

Field	Definition
Event Name	Name of the event.
Group	Group name of a group of elements, such as port group, device group or user group used to limit generation of the selected event to the items in the group. If set to All Groups, then the event is generated for all items, such as ports, devices, hosts or users. If no group is displayed, an event is generated for the system, and not a specific item.
Group Type	Indicates whether this event applies to a group of ports, devices, hosts, users or administrators.
Last Modified By	User name of the last user to modify the event.
Last Modified Date	Date and time of the last modification to this event.
Right click options	
Modify Group	Opens the Modify Group window.
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746 .
	 You must have permission to view the admin auditing log. See Add an administrator profile on page 139.
Disable Logging	Disables the event is disabled. The event will not be generated or logged anywhere.
Log Internal	Logs the event only to an internal events database.
Log External	Logs the event only to an external host.
Log Internal & External	Logs the event to both an internal events database and an external host.
Buttons	
Options	Allows you to change the log or group setting for one or more selected events.
Modify Group	Change the group setting for one or more selected events.

Enable and disable events

Use the event management window to select which events will be logged.

Events for the system

1. Click **Logs > Events & Alarms > Management**.
2. Use the Filters to locate the appropriate event. Refer to [Event management on page 772](#) for filter settings.
 - a. To enable an event, select one or more events and click **Options**. Select one of the following:
 - **Internal**: Logs only to an internal events database.
 - **External**: Logs only to an external host.
 - **Internal & External**: Logs both to an internal events database and an external host.
 Any event that is logged is enabled.
 - b. To disable an event, select one or more events and click **Options**. Select **Disable Logging**.

To log events on an external log host, you must first add the log host to FortiNAC. See [Log events to an external log host on page 776](#) for instructions.

Events for a specific group

Logging events for a specific group limits the number of times the event is generated. The event will only be generated for members of the selected group.

1. Click **Logs > Events & Alarms > Management**.
2. Use the filters to locate the appropriate event. Refer to [Event management on page 772](#) for filter settings.
3. Select one or more events and click **Options**. Choose one of the logging options to enable the event.
4. Click **Modify Group**.
5. Click in the **Group** drop-down box and select the group for which this event will be enabled.
6. Click **OK**.

Event thresholds

This option allows you to monitor license usage, memory usage, process thread counts, and disk space, and establish thresholds for the processes and hard drives. Each process type has its own thread count and maximum memory allocations. The percentages in the thresholds are not relative to the total memory available on the appliance; they are relative to the maximum amounts of memory that each loader process is allowed to consume.

View the memory allocated to each process in the Performance panel on the dashboard. The number of threads used by the process is also contained in the panel. See [System Performance on page 94](#).

When a threshold is exceeded, an event is generated. Each event has an associated alarm which is mapped by default. Each specific event or alarm mapping is configured so that multiple events for a specific process or threshold results in a single alarm. Modify the default mappings in Event to Alarm Mappings. You can also configure a specific action, such as email notification. See [Map events to alarms on page 784](#) for details.

Settings

Threshold	Description
License thresholds	

Threshold	Description
Concurrent Licenses Warning/Critical	Generated when the license usage threshold is reached. This threshold is a percentage of the total number of licenses configured. Default Warning = 75%. Default Critical = 95%.
Hardware thresholds	
Hard Disk Usage Warning / Critical	Generated when the disk usage threshold is reached. This threshold is a percentage of the space allocated for the bsc and var partitions. The percentage is calculated for each partition separately. When any one partition reaches the threshold the event is generated. Thresholds calculated for individual partitions are never combined. Therefore if the combined total crosses the threshold, no event is generated. Default Warning = 85%. Default Critical = 95%.
Memory Usage Warning / Critical	Generated when the memory usage threshold is reached for the appliance. This threshold is a percentage of the total allocated memory. Default Warning = 85%. Default Critical = 95%.
Network Topology Size Warning / Critical	Generated when the system sizing tool detects that the appliance has reached the threshold for possible connections. This threshold is a percentage of the total connections that the appliance can manage. Default Warning = 85%. Default Critical = 95%.
Software thresholds	
Process Thread Count Warning / Critical	Generated when the process thread count threshold is reached. This threshold is a specific number of threads the process is using. MasterLoader: Default Warning = 500. Default Critical = 575. Nessus: Default Warning = 100. Default Critical = 125.
Process Memory Usage Warning / Critical	Generated when the memory usage threshold is reached for the process. This threshold is a percentage of the total allocated memory. Default Warning = 85%. Default Critical = 95%.

Set thresholds for self-monitoring events

1. Click **Logs > Events & Alarms > Management**.
2. Click the **Event Thresholds** button at the top of the window.
3. Click the **License Tab**. Enter the value for the warning and critical levels of the license usage.
4. Click the **Hardware Tab**. Enter the value for the warning and critical levels of the hardware thresholds for hard disk and memory usage.
5. Click the **Software Tab**. Enter the value for the warning and critical levels of the software thresholds for each system process.
6. Click **OK**.

Log events to an external log host

To log events on an external log host, you must first add the log host to the Log Receivers View. Once you have added the log host server, configure the events to be logged externally on the Event Management View. The events will be sent as Syslog messages, SNMP Traps, or FortiAnalyzer OFTP (Fortinet proprietary format).

Add a server

1. Click **System > Settings**.
2. In the tree on the left select **System Communication > Log Receivers**.
3. Click **Add** to add a log host.
4. Select the type of server.
5. Enter the IP address of the server.
6. Enter the configuration parameters for the type of log host. The standard port information for each host type is automatically entered. See the table below for detailed information on each type of server.
7. Click **OK**.

Settings

Field	Definition
Type	Type of server that will receive Event and Alarm messages. Options include: Syslog CSV, SNMP Trap, FortiAnalyzer OFTP, and Syslog Command Event Format (CEF).
IP address	IP address of the server that will receive Event and Alarm messages.
Port	Connection port on the server. For Syslog CSV and Syslog CEF servers, the default = 514. For SNMP Trap servers the default = 162

Field	Definition
Facility	Displays only when Syslog is selected as the Type. Allows you to configure the message type. The default is 4. Options include: • 0 kernel messages • 1 user-level messages • 2 mail system • 3 system daemons • 4 security/authorization messages • 5 messages generated internally by syslogd • 6 line printer subsystem • 7 network news subsystem • 8 UUCP subsystem • 9 clock daemon • 10 security/authorization messages • 11 FTP daemon • 12 NTP subsystem • 13 log audit • 14 log alert • 15 clock daemon • 16 local use 0 (local0) • 17 local use 1 (local1) • 18 local use 2 (local2) • 19 local use 3 (local3) • 20 local use 4 (local4) • 21 local use 5 (local5) • 22 local use 6 (local6) • 23 local use 7 (local7)
Security String	Displays only when SNMP is selected as the Type. The security string sent with the Event and Alarm message.

Configure events to log externally

1. Click **Logs > Events & Alarms > Management**.
2. Use the filters to locate the appropriate event. Refer to [Event management on page 772](#) for filter settings.
3. For each event that should be logged externally, select one or more events and click **Options**. Select one of the following:
 - **External**: Logs only to an external host.
 - **Internal & External**: Logs both to an internal events database and an external host.

Syslog format

The following is an example of a syslog message:


```
<37>Apr 10 11:42:16 : 2009/04/10 11:42:16 EDT,3,2587,Probe - MAP IP To MAC
Success,0,1127,,BuildingB-3750,192.168.10.1,,Successfully read IP address mappings
from device BuildingB-3750
```

Format

Column	Data From Example	Definition
1	<37>	Syslog category: This is the defined facility and the severity Default Facility = 4 Security message Severity = 5 Notice
2	Apr 10 11:42:16 :	Time of the syslog generation.
3	2009/04/10 11:42:16 EDT	Log time.
4	3	Log type: • 1 Event • 2 Alarm • 3 Security Alarm
5	2587	Database ID AlarmID or ElementID
6	Probe - MAP IP To MAC Success	Name of the event that generated the syslog message.
7	0	Severity: • 0 Normal • 1 Minor • 2 Major • 3 Critical
8	1127	Entity ID
9		Unique Identifier (user ID)
10	BuildingB-3750	Entity Name
11	192.168.10.1	Entity IP address
12		Entity physical address
13	Successfully read IP address mappings from device BuildingB-3750	Log Message

SNMP trap format

The following is an example of an SNMP message:

```
1.3.6.1.4.1.16856.1.1.5="2009/04/10 11:37:02 EDT", 1.3.6.1.4.1.16856.1.1.6=1,
1.3.6.1.4.1.16856.1.1.7=2585, 1.3.6.1.4.1.16856.1.1.8="Probe - MAP IP To MAC
Success", 1.3.6.1.4.1.16856.1.1.9=0, 1.3.6.1.4.1.16856.1.1.10=1127,
1.3.6.1.4.1.16856.1.1.15=, 1.3.6.1.4.1.16856.1.1.11=BuildingB-3750,
1.3.6.1.4.1.16856.1.1.12=192.168.10.1, 1.3.6.1.4.1.16856.1.1.13=,
1.3.6.1.4.1.16856.1.1.14="Successfully read IP address mappings from device
BuildingB-3750."
```

Format

MIB Object	Data From Example	Definition	Data Type
1.3.6.1.4.1.16856.1.1.5	"2009/04/10 11:37:02 EDT"	The log time stamp in the format YYYY/MM/DD hh:mm:ss z	Counter32
1.3.6.1.4.1.16856.1.1.6	1	The type of log message 1 - Event message 2 - Alarm Message	Counter32
1.3.6.1.4.1.16856.1.1.7	2585	The database identifier of the log message	String
1.3.6.1.4.1.16856.1.1.8	"Probe - MAP IP To MAC Success"	Name of the event that generated the syslog message.	Counter32
1.3.6.1.4.1.16856.1.1.9	0	The log severity 0 - Normal 1 - Minor 2 - Major 3 - Critical	Counter32
1.3.6.1.4.1.16856.1.1.10	1127	The database identifier of the log entity	String
1.3.6.1.4.1.16856.1.1.15		The unique identifier of the log entity "User ID"	Counter32
1.3.6.1.4.1.16856.1.1.11	BuildingB-3750	The textual name of the log entity	Counter32
1.3.6.1.4.1.16856.1.1.12	192.168.10.1	The IP address of the log entity. The format is 0.0.0.0"	Counter32
1.3.6.1.4.1.16856.1.1.13		The Physical address of the log entity. The format is 00:00:00:00:00:00"	Counter32
1.3.6.1.4.1.16856.1.1.14	"Successfully read IP address mappings from device BuildingB-3750."	The textual log message	Counter32

Common event format (CEF)

Fields contained within a CEF syslog message include:

```
CEF:Version|Device Vendor|Device Product|Device Version|Signature
ID|Name|Severity|Extension
```

Example:

```
<37>Jul 22 11:24:20 : CEF:0|Fortinet|NAC Control Server|4.1.1.219.P9|6111|Login
Failure|1|rt=Jul 22 11:24:20 602 EDT cat=Network shost=NAC Director msg=User qa
failed to log in.
```

Format

Column Title	Data From Example	Definition
Facility	<37>	Syslog category: This is the defined facility and the severity Default Facility = 4 Security message Severity = 5 Notice This is not part of the CEF format, but is contained within the syslog message.
Date/Time	Jul 22 11:24:20	Date and time the syslog message was generated. This is not part of the CEF format but is contained within the syslog message.
CEF: Version	CEF:0	Version number defines the fields that are expected to follow this field.
Device Vendor	Fortinet	These fields uniquely identify the type of device sending the syslog message. In this case, the sending entity is FortiNAC.
Device Product	NAC Control Server	
Device Version	4.1.1.219.P9	
Signature ID	6111	Unique identifier per event type. This can be a string or an integer.
Name	Login Failure	Name of the event that generated the syslog message.
Severity	1	Severity: 0 Normal 1 Minor 2 Major 3 Critical
Extension	rt=Jul 22 11:24:20 602 EDT cat=Network shost=NAC Director msg=User qa failed to log in.	Extension is a place holder for additional data. The extensions contained in this message include:

Column Title	Data From Example	Definition
		rt - receiptTime - Time stamp that indicates when the event was generated. cat -category-Type of device sending the syslog message. msg - message- Message giving more details about the event.

Examples of syslog messages

Here are some examples of syslog messages that are returned from FortiNAC. In these examples, the Syslog server is configured as follows:

- Type: Syslog
- IP address: a.b.c.d
- Port: 514
- Facility: Authorization

Event	Description	Syslog Message
Login Success	This is the event that is logged with a user logs into the admin UI.	02-28-2014 08:16:04 Auth.Notice 192.168.34.31 Feb 27 22:16:14 : 2014/02/27 22:16:14 EST,1,545570,Login Success,0,12,,,,,User root logged in.
Map IP To MAC Failure	This is a legacy event logged when a scheduled task runs (these are no longer used for IP-MAC) and the ARP is not read.	--
Probe - Map IP To MAC Failure	This is the event when we fail to poll and L3 device for IP->MAC (reading Arp Cache) L3 Polling	02-28-2014 09:00:14 Auth.Notice 192.168.34.31 Feb 27 23:00:24 : 2014/02/27 23:00:24 EST,1,545702,Probe - MAP IP To MAC Failure,0,28,,Switch,192.168.34.1,,Failed to read IP address mappings from device Switch.
User Logged Out	This is the event that is logs when a user logs out of the admin UI.	02-28-2014 08:48:55 Auth.Notice 192.168.34.31 Feb 27 22:49:04 : 2014/02/27 22:49:04 EST,1,545670,User Logged Out,0,12,,,,,User root Logged Out.
User Logged off Host	This event is logged when a user logs off a host	02-28-2014 08:44:25 Auth.Notice 192.168.34.31 Feb 27 22:44:34 : 2014/02/27 22:44:34 EST,1,545655,User Logged off Host,0,4155,,,,,"User Man, Bat logged off session 1 on host BRADSUPP7-LT"
User Logged onto Host	This event is logged when a user logs onto a host	02-28-2014 08:37:58 Auth.Notice 192.168.34.31 Feb 27 22:38:07 : 2014/02/27 22:38:07 EST,1,545633,User Logged onto Host,0,4155,,,,,"User Man, Bat logged onto session 1 on host BRADSUPP7-LT"

Event	Description	Syslog Message
User Remotely Connected to Host	An event that is logged when a user remotely connected to a terminal session on a host using the PA	--
User Locked Session	This event is logged when a user locks his workstation	02-28-2014 08:49:53 Auth.Notice 192.168.34.31 Feb 27 22:50:03 : 2014/02/27 22:50:03 EST,1,545681,User Locked Session,0,4155,,,,,"User Man, Bat locked session 2 on host BRADSUPP7-LT"
User Unlocked Session	This event is logged when a user unlocks his workstation	02-28-2014 08:52:07 Auth.Notice 192.168.34.31 Feb 27 22:52:16 : 2014/02/27 22:52:16 EST,1,545691,User Unlocked Session,0,4155,,,,,"User Man, Bat unlocked session 2 on host BRADSUPP7-LT"

View events currently mapped to alarms

1. Select **Logs > Events & Alarms > Mappings**. The Event to Alarm Mappings view appears.
2. To add a new mapping see [Add or modify alarm mapping on page 787](#) for instructions.

Alarms

Use **Alarms** to view and manage the contents of the alarm log. The alarm log is a list of all current alarms. The Severity column indicates how serious the alarm is. Severity levels include: critical, minor, warning, informational.

The state of an alarm is either acknowledged or not acknowledged. The event-to-alarm mapping determines the behavior and characteristics of the alarm. The event-to-alarm mapping feature gives you the option of sending alarms to an external log host. See [Map events to alarms on page 784](#) for details.

You can remove alarms from the log in two ways:

- Manually, when you select and clear the alarm
- Automatically, when the clear event defined in alarm mapping occurs

To access the alarms view, select **Logs > Events & Alarms > Alarms**.

Settings

Field	Definition
First Name	First Name of the user associated with the alarm, such as the registered owner of a host or an administrator.
Last Name	Last Name of the user associated with the alarm.
User ID	User name from the credentials of the user who was logged in and associated with the alarm.
Element Name	Name of the device, administrator, server or process associated with the alarm.
Element Type	Type can be Device, Port, Container, Process, or All.
Group	Group name of a group of elements, such as port group, device group or user group.
Pause	If enabled, prevents the Alarms List from refreshing and adding new records to the screen. In an environment with a large number of alarms, you may need to pause the refresh in order to research an issue.
Severity	Category indicating how serious the alarm is. Options include: Critical, Minor, Warning and Informational
Date	Date and time the alarm was triggered.
Alarm	Alarm name. See Events and alarms list on page 750 .
Element	Element associated with the alarm entry, such as a user name, a hostname, a switch name or an application name.
Trigger Rule	Rule that determine the conditions under which an alarm is triggered based on an event. Options include: • One Event to One Alarm: Every occurrence of the event generates a unique alarm. • All Events to One Alarm: The first occurrence of the event generates a unique alarm. Each subsequent occurrence of the event does not generate an alarm, as long as the alarm persists when subsequent events occur. When the alarm clears, the next occurrence of the

Field	Definition
	event generates another unique alarm. • Event Frequency: Number of the occurrences of the event generated by the same element within a user specified amount of time determines the generation of a unique alarm. • Event Lifetime: Duration of an alarm event without a clearing event within a specified time, determines the generation of a unique alarm.
Acknowledged Date	Indicates the date the alarm was acknowledged. If this field is blank, it indicates that the alarm was never acknowledged.
Buttons	
Import	Import historical records from an Archive file. See Import archived data on page 102 .
Acknowledge	Acknowledges the selected alarm but does not clear it. The Alarm remains in the displayed until you clear it. A date is displayed in the Acknowledged column when the alarm is acknowledged.
Delete	Clears the selected alarm and removes it from the list.
Show Details	Displays the Details Panel for the selected alarm. See Show or hide alarm details on page 784 .

Show or hide alarm details

The Alarm Details panel launched from the Alarms View displays a detailed narrative about the cause of the selected alarm and the event that triggered it. For example, if there is an alarm indicating that an L2 Poll failed, the possible causes are displayed indicating that the security string may be incorrect or the telnet credentials are incorrect. This gives the administrator two things to verify when trying to correct the problem.

1. Select **Logs > Events & Alarms > Alarms**.
2. Use the filters to locate the appropriate alarm. Refer to [Alarms on page 783](#) for settings.
3. Select the alarm.
4. Click **Show Details**.
5. Review the details displayed.
6. Click **Hide Details** to close the panel.

Map events to alarms

An event indicates that something significant has happened within FortiNAC. All events that are generated are logged in the event log. If an event is mapped to an alarm, you are immediately informed by the alarm notification system. Some events are mapped to alarms by default.

To view events that are mapped to alarms select **Logs > Events & Alarms > Mappings**. For a list of possible alarms see [Events and alarms list on page 750](#).

If an event is disabled, the associated Alarm Mapping is grayed out and has a line through it. To enable the event, right click on the Alarm Mapping and select one of the Enable options.

Enable/disable alarm mappings

When mapping events to alarms, you have the option to disable an alarm mapping to prevent the generation of alarms when the selected event occurs. This may be useful during periods you know will generate many events. An example of this is during the repair of a modeled network device. You may want to block the Device Contact Lost and Established events from getting to the system since they will be expected. Another example is to block the Rogue User Detected event during an Open House when many rogues will be detected. Use **Enable** and **Disable** at the top of the view to enable and disable selected alarm mapping records.

Settings

Refer to [Add or modify alarm mapping on page 787](#) for additional information on each field.

Field	Definition
Enable Buttons	Enables or disables the selected Alarm Mappings. Disabled mappings do not trigger an alarm when the associated event is generated.
Enabled	A green check mark indicates that the mapping is enabled. A red circle indicates that the mapping is disabled.
Event	Name of the Event that triggers this alarm.
Alarm	Name of the Alarm that is mapped to the event.
Clear Event	Name of the event that must be generated to clear the alarm mapped in this Alarm and Event combination.
Severity	Critical, Minor, Warning, or Informational. Only the text of the severity is displayed. Severity icons do not display in the Alarm Mappings table.
Notify Users	Indicates who will be notified if this alarm is triggered, such as All Management group.
Trigger Rule	Rules that determine when the alarm is triggered. Options include: • One Event to One Alarm: Every occurrence of the event generates a unique alarm. • All Events to One Alarm: The first occurrence of the event generates a unique alarm. Each subsequent occurrence of the event does not generate an alarm, as long as the alarm persists when subsequent events occur. When the alarm clears, the next occurrence of the event generates another unique alarm. • Event Frequency: Number of the occurrences of the event generated by the same element within a user specified amount of time determines the generation of a unique alarm. • Event Lifetime: Duration of an alarm event without a clearing event within a specified time, determines the generation of a unique alarm.
Apply To	Elements to which this alarm mapping applies. Options include: • All: Applies this mapping to all elements. • Group: Applies this mapping to a single group of elements. • Specific: Applies this mapping to an element that you select from a list.

Field	Definition
Action	If an Action is enabled in the mapping, displays the action that will be taken when this alarm is triggered. Options include: • Host Access Action: Host is disabled and then re-enabled after the specified time has passed. • Host Role: The host's role is changed and then set back to the original role after the specified time has passed. • Host Security Action: Host is set At Risk and then set to Safe after the specified time has passed. • Command Line Script: You can specify a particular command line script to be executed as an alarm action. • Email User Action: An email is sent to the user associated with the host. • SMS User Action: An SMS Message is sent to the user associated with the host. • Port State Action: Port is disabled and then re-enabled after the specified time has passed. • Send Message to Desktop: Send a text message to the desktop of a host(s) with the Persistent Agent or Mobile Agent installed.
Send To External Log Hosts	Indicates whether this alarm is sent to an external log host when the trigger event occurs, select this check box. Default = No. To configure remote hosts that will receive externally logged alarms, see Log receivers on page 938.
Send To Custom Script	Name of the command line script to be executed when this alarm is triggered. These command line scripts are for advanced use, such as administrator-created Perl scripts. Scripts are stored on the server in the following directory: <code>/home/cm/scripts</code> The script will receive one packed argument that the script can parse for the desired data. Example 'type="Network" name="FortiNAC" msg="Alarm Admin User Login Failure asserted on FortiNAC Mon Feb 27 14:34:35 EST 2017. The following Events caused the Alarm. Admin user efewfwf failed to log in. Admin user efewfwf failed to log in. Admin user efewfwf failed to log in. "'
Event Logging	Indicates where the event is being logged or if logging has been disabled. Options include: • Disabled: Event is disabled and will not be generated or logged anywhere. • Internal: Logs only to an internal events database. • External: Logs only to an external host. • Internal & External: Logs both to an internal events database and an external host.
Event Logging Group	Group name of a group of elements, such as port group, device group or user group used to limit generation of the selected event to the items in the group. If set to All Groups, then the event is generated for all items, such as ports, devices, hosts or users.

Field	Definition
Last Modified By	User name of the last user to modify the mapping.
Last Modified Date	Date and time of the last modification to this mapping.
Right click options	
Delete	Deletes selected mappings from the database.
Modify	Opens the Modify dialog and allows you to modify the selected mapping. When multiple mappings are selected, opens a limited Modify dialog and allows you to modify Severity and Notification settings. See Bulk modify alarm mappings on page 791 .
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746 .
 You must have permission to view the admin auditing log. See Add an administrator profile on page 139.	
Enable	Enables the selected mappings.
Disable	Disables the selected mappings.
Event Logging - Disable	Disables the events associated with the selected mappings.
Event Logging - Internal	Enables the events associated with the selected mappings and logs to an internal events database.
Event Logging - External	Enables the events associated with the selected mappings and logs to an external host.
Event Logging - Internal & External	Enables the events associated with the selected mappings and logs to both an internal events database and an external host.
Export	Exports data to a file in the default downloads location. File types include CSV, Excel, PDF, or RTF. See Export data on page 116 .

Add or modify alarm mapping

1. Select **Logs > Events & Alarms > Mappings**.
2. Click **Add** or double-click on an existing mapping to modify it.
3. Refer to the table below for detailed information about each field.
4. The new mapping is enabled by default. If you wish to disable it, remove the check mark from the **Enabled** check box.
5. In the **Apply To** section, select the element affected by this mapping. You can apply mappings to all elements, a single group of elements, or specific elements.
Available selections vary depending upon the selected trigger event.
6. Click the box and select an element from the drop-down list.

7. If you choose to **Apply To a Group**, you can select a group from the list or use the icons next to the group field to add a new group or modify the group shown in the drop-down list. Note that if you modify a group, it is modified for all features that make use of that group. See [Add groups on page 845](#) for additional information.
8. Select the **Notify Users** settings.
9. If you choose to notify users, you can select an admin group from the list or use the icons next to the **Group** field to add a new group or modify the group shown in the drop-down list. Note that if you modify a group, it is modified for all features that make use of that group. See [Add groups on page 845](#) for additional information.
10. Select the **Trigger Rule** for the event from the drop-down list. Rules determine when an Event triggers the creation of an Alarm.
11. If you enable the **Action** option, select the **action** to take when the event occurs and the alarm is asserted. These are basic actions that FortiNAC executes on a given alarm.
12. Action parameters display. Select the **Primary Task** from the drop-down list.
13. For some actions there is a secondary task. If desired, click the **Enable** box in the **Run Secondary Task** section, select **Min**, **Hr**, or **Day** and enter the corresponding value.
14. Click **OK**. The new mapping is saved and appears in the **Event/Alarm Map View**.

Settings

Field	Definition
Alarm definition	
Enabled	If checked, the alarm mapping is enabled. Default = Enabled.
Trigger Event	Event that causes the alarm. Whenever this event occurs, its associated alarm is generated. The alarm is automatically listed when you select the event.
Alarm to Assert	The alarm generated when the event occurs.
Severity	Sets the severity of the alarm. Select one of the values from the drop-down list: Critical, Informational, Minor, and Warning. This value may be changed for existing Alarm and Event mappings.
Clear on Event	To automatically clear the alarm when a specific event occurs, select this check box. Select the event that, when generated, causes this alarm to be removed. If you leave the check box unchecked, you must manually clear the alarm. Default = Unchecked (Disabled)
Send Alarm to External Log Hosts	The alarm is sent to an external log host when the trigger event occurs, select this check box. See Log receivers on page 938 for details on configuring an external log host. Default = Unchecked (Disabled)
Send Alarm to Custom Script	You can specify a particular command line script to be executed when this alarm is triggered. These command line scripts are for advanced use, such as administrator-created Perl scripts. First, write the script that is to be used as the alarm action. Store the script in this directory: <code>/home/cm/scripts</code> If there are no scripts in the directory, this field is not available. Click the check box to enable the option and select the correct script from the drop-down list. The arguments that are automatically passed to the script are as follows:

Field	Definition
	• type: EndStation. User or network device • name: name of element • ip: IP address • mac: MAC address • user: userID • msg: email message from alarm
Apply To	• All: Applies this mapping to all elements. • Group: Applies this mapping to a single group of elements. • Specific: Applies this mapping to the element that you select from a list.
Notify users	
Notify	If checked, the administrators in the selected group are notified when an alarm occurs.
Send Email	If checked, the administrators in the selected group are sent an email when the alarm occurs. Administrators must have an email address configured in the Modify User dialog to receive this email.
Send SMS	If checked, the administrators in the selected group are sent an SMS message when an alarm occurs. Administrators must have a Mobile Number and Mobile Provider configured to receive this SMS message.
Trigger rules	
One Event to One Alarm	Every occurrence of the event generates a unique alarm.
All Events to One Alarm	The first occurrence of the event generates a unique alarm. Each subsequent occurrence of the event does not generate an alarm, as long as the alarm persists when subsequent events occur. When the alarm clears, the next occurrence of the event generates another unique alarm.
Event Frequency	The number of the occurrences of the event generated by the same element within a user specified amount of time determines the generation of a unique alarm. Settings are updated when the Action is configured. Example: Assume the host connected event is mapped to an alarm and the frequency is set to 3 times in 10 minutes. • Host A connects 3 times in 10 minutes and the alarm is triggered. • Host A connects 2 times and host B connects 2 times, there are 4 connections in 10 minutes. No alarm is generated because the hosts are different. • Host A connects at minutes 1, 8 and 12. No alarm is triggered because the host did not connect 3 times in 10 minutes. • Host A connects at minutes 1, 8, 12, and 14. An alarm is triggered because connections at minutes 8, 12 and 14 fall within the 10 minute sliding window.

Field	Definition
Event Lifetime	The duration of an alarm event without a clearing event within a specified time, determines the generation of a unique alarm. Example: Event A occurs. If Event B (clear event) does not occur within the specified time, an alarm is generated.
Actions	
Action	If checked, the selected action is taken when the alarm mapping is active and the alarm is asserted.
Host Access Action	Host is disabled and then re-enabled after the specified time has passed.
Host Role	The host's role is changed and then set back to the original role after the specified time has passed. Roles are attributes of the host and are used as filters in user/host profiles. Those profiles determine which network access policy, endpoint compliance policy or Supplicant EasyConnect Policy to apply. If roles are based on a user's attribute from your LDAP or Active Directory, this role change is reversed the next time the directory and the FortiNAC database resynchronize.
Host Security Action	Host is set At Risk and then set to Safe after the specified time has passed.
Command Line Script	You can specify a particular command line script to be executed as an alarm action. These command line scripts are for advanced use, such as administrator-created Perl scripts. First, write the script that is to be used as the alarm action. Store the script in this directory: <code>/home/cm/scripts</code> The IP and MAC address arguments that are automatically passed to the script are in the format shown in this example: <pre>/home/cm/scripts/testScript 192.168.10.1 00:00:00:00:00:00</pre>
Email User Action	An email is sent to the user associated with the host. The text of the email is entered in the Email Host Action dialog box. HTML tags may be added to text within the content of the email in order to format the text, convert the text to a link, etc. For example, you can add the <code></code> and tags to text in the Email message window to bold the selected text in the recipient's email message.
SMS User Action	An SMS Message is sent to the user associated with the host. The text of the message is entered in the SMS User Action dialog box. The recipient must have a Mobile Number and Mobile Provider configured.
%host%	Allows you to include information specific to the non-compliant host in the email or SMS alert message. For example, this message:

Field	Definition
	The system referenced below has been found at risk. Please contact your Help Desk for assistance in remediating this issue. %host% is displayed as: The system referenced below has been found at risk. Please contact your Help Desk for assistance in remediating this issue: Host: Host Name: TestUser-MacBook-Pro-2 OS: macOS 10.7.5 Network Adapters: Connected 3C:07:54:2A:88:6F, 192.168.10.143, Concord-3750 Fa3/0/46 Disconnected 60:C5:47:8F:B1:66, 192.168.4.70, Concord_Cisco_1131.example.com VLAN 4
%event%	Allows you to include information specific to the event in the email or SMS alert message. For example, this message: The system referenced below has been found at risk. Please contact your Help Desk for assistance in remediating this issue: %event% is displayed as: The system referenced below has been found at risk. Please contact your Help Desk for assistance in remediating this issue: Host failed Test-Host Tests: Failed :: Anti-Virus :: ClamXav MAC address: 3C:07:54:2A:88:6F Last Known Adapter IP: 192.168.10.143 Host Location: Concord-3750 Fa3/0/46 . Remediation Delayed.
Port State Action	The port is disabled and then re-enabled after the specified time has passed.
Send Message to Desktop	Send a text message to the desktop of a host(s) with the Persistent Agent or Mobile Agent installed.

Bulk modify alarm mappings

This option displays on the right-click menu only when multiple mappings are selected in the Event to Alarm Mappings View. It provides a limited Modify dialog with options to modify Severity and Notification settings.

1. Select **Logs > Events & Alarms > Mappings**.
2. Use Ctrl or Shift to select multiple alarm mappings.
3. Right-click on the selected records and choose **Modify** from the pop-up menu.

4. Use the table below to modify the selected mappings.

Field	Definition
Severity	Enables the Severity drop-down. The severity level of the alarm. Options include: Critical, Informational, Minor and Warning.
Notify Users	Enables the Notify Users settings.
Notify Group	Drop-down list of Admin groups. Use this to determine who will be notified when this alarm is triggered. The default is the All Management group which contains all administrators.
Send Email	If enabled, administrators in the selected group receive an email when this alarm is triggered.
Send SMS	If enabled, administrators in the selected group receive a text message when this alarm is triggered. Administrators must have a mobile phone number and a mobile provider listed on their user records to receive SMS messages.

5. Click **OK** to save your changes.

Delete alarm mapping

1. Select **Logs > Events & Alarms > Mappings**.
2. Select the appropriate mapping record from the list displayed.
3. Click **Delete**.
4. At the prompt, click **OK**.

Reports

Use reports to see standard reports and to create custom reports based on the information in the database. The report data may be output to HTML, CSV, EXCEL, XML, RTF, and PDF formats.

The template reports include: guest registration, registration, and scan results. You can set the schedule for the standard reports and preview the results prior to scheduling, including sections of the report related to failures.

Custom reports include: registrations, registration failures, scan results, and connection logs. For custom reports, configure the report by selecting parameters, filters, scheduling, and type of output. You can import the output files into other report generation tools.

Archives include reports that have been run based on a scheduled task and are archived for you to view at your convenience. You can schedule both standard and custom reports to run at a particular time and be sent via email to an administrator group.

Standard report templates

Use the Templates tab to access standard Guest Registration, Registration and Scan Results reports. The Guest Registration report includes information on Guests/Contractors that have logged into the system. The Registration reports include statistics on successful and failed attempts to register and login errors. The scan results reports include endpoint compliance policy scan results information.

You can schedule these reports to be sent to an Administrator group. The email contains graphical data as well as tabular data in report form. See [Schedule reports on page 802](#) for details.

To access this window select **Logs > Reports**, select **Templates** on the left.

Preview standard report templates

Use the Preview Settings section to see the report that will be generated from the report parameters you have selected. If the results are acceptable, enter the parameters into the report schedule view.

1. Select **Logs > Reports**.
2. Select **Templates** from the menu.
3. Select the **Report Type**.
4. Enter the number of hours, days, or weeks in the **Data** range field and select the range from the drop down list.
5. Enter the range end time in the format MM/DD/YY hh:mm AM/PM.
6. Click **Preview**.
7. Click **Details** to view additional information.

Guest registrations report

This report provides you with a list of guest accounts created between the specified dates. See [Preview standard report templates on page 793](#) for instructions on generating this report.

When the report has multiple pages, use the **[First/Prev]** or **[Next/Last]** options to view the pages of the report, or click a page number to view a specific page.

Settings

Field	Definition
Start Time	Start time and date of the report. This time is automatically set to one month prior so that you can see guest or contractor accounts and registrations for a month.
End Time	End time and date are set automatically to the time and date that you view the report.
Sponsor	Sponsor that created the guest or contractor account.
Type	Type of user, such as guest or contractor.
User	User's email address.
Name	Name of the user.
Starting	Account start date and time.
Ending	Account end date and time.
Availability	Times and days that the user can log into their account.
Role	Role of the user. For more on roles, see Roles on page 620 .
Max Registrations	Maximum number of registrations that can be made on this account. For example, a conference with the same username and password for all attendees requires that all register under the same account.
Total Registrations	Total number of hosts that have been registered for each account.
Details	View additional information about the guest, including additional data fields that were added to the Guest, Contractor, or Conference template. The details appear only if the guest is registered.
Export Options	To export this report click an output format and follow the instructions to save the file at the desired location. The available options are: CSV, Excel, XML, PDF, RTF.
Details	
User	Guest user name. Typically this is the guest's email address.
Registration Time	Date and time that the guest registered his computer on the network. This would be the first time that the guest accessed the guest account.
Email First Name Last Name Phone Address City State Zip/Postal Code	Guest's demographic information.
Location	Switch and port where the guest last connected to the network.
Host Name	Name of the host the guest registered on the network.
Operating System	Operating system of the host the guest registered on the network.

Registrations report

This report provides you with the number of host registrations by operating systems between the specified dates. See [Preview standard report templates on page 793](#) for instructions on generating this report.

Settings

Field	Description
Start Time	Start time and date of the report selected when the report was requested.
End Time	End time and date are set automatically to the time and date that you view the report.
Failures	Number of failed registrations. If the same user has failed to register his host more than once, each failure increments the total count.
Registrations	Number of successful registrations.
OS	Total successful registrations by operating system.
Failure Description	Reasons for failed registrations and the number of occurrences of each reason.
Details	
OS	Total successful registrations by operating system. Only displays those operating systems for which there were registrations.
User	User name of the network user who attempted to register and failed.
Failure Description	Reason that the user failed to register his host.
Total	Total number of failed registration attempts for each user/failure reason combination.

Scan results report

The Scan Results Report provides Success and Failure rates for each Scan in your database. Data is broken out by operating system. See [Preview standard report templates on page 793](#) for instructions on generating this report.

Note that a host may be scanned more than once, particularly if it does not pass the scan the first time. Each time a host is scanned the totals are incremented. For example, if a host was scanned and failed nine times and then scanned and passed once, the Success total is incremented by one, the Failure total is incremented by nine, the total for the Scan name is incremented by ten and the total for all scans is incremented by ten.

Typically, a host will not be evaluated against more than one Scan unless something about that host changes. For example, assume you have a user who is typically at a desk and is assigned an endpoint compliance policy for employees. The user is invited to a meeting and goes to a different corporate building. When he connects to a switch there, he is assigned a different policy based on his new connection location. In a case like this a host might be counted in more than one scan because it was indeed evaluated by two different Scans contained within two different endpoint compliance policies.

As you drill down into the details windows the report becomes more and more granular causing the totals to increase. In the samples shown below the Default scan starts out with 40 scans. However, as the individual requirements for each scan are counted the numbers increase to 2580. For any given scan you can require antivirus. Within those categories you can indicate what the preferred software is. For example, your company may prefer that users have AVG on their hosts but allow several other brands of antivirus software. If a user has no antivirus software on his host, the host fails

the scan for the preferred antivirus. The number of failures for the preferred antivirus does not indicate the number of hosts with no antivirus. It simply indicates the number of times a scan ran and failed. The same host could have been scanned and failed multiple times.

Scan results settings

Field	Definition
General	
Start Time	Start time and date of the report selected when the report was requested.
End Time	End time and date are set automatically to the time and date that you view the report.
Scan list	
Policy	Name of the scan used to evaluate the host.
Type	Type of scan engine. Types include: System, Nessus, Admin and Agent. Agent scans are run using the Persistent Agent, Mobile Agent, Dissolvable Agent, or the Passive Agent. For information on System, Nessus and Admin Scans see Add a scan on page 616 .
Success	Number of times hosts passed the scan. This scan may have been run on the same host more than once. Each time a scan is run it increments the totals.
Failure	Number of times hosts failed the scan. This scan may have been run on the same host more than once. Each time a scan is run it increments the totals.
Totals	Totals for Successful scans, Failed scans and all scans performed within the time range you selected.
Details Button	Click to display additional details about a specific Scan.
OS	Total scans broken down by host operating system.

Scan details settings

Field	Definition
General	
Start Time	Start time and date of the report selected when the report was requested.
End Time	End time and date are set automatically to the time and date that you view the report.
OS list	
Type	Type of scan engine. Types include: System, Nessus, Admin and Agent. Agent scans are run using the Persistent Agent, Dissolvable Agent, or the Passive Agent. For information on system, Nessus, and admin scans, see Add a scan on page 616 .
Totals	Total number of scans broken down by host operating systems using the policy selected in the previous page. This does not indicate the number of hosts scanned because a single host could be scanned more than once.
Scan categories	

Field	Definition
Type	Indicates the type of scan engine used to scan the host.
Category	Lists categories included in the selected policy for which the engine is scanning, such as operating system or antivirus. This indicates that there are requirements in the policy for these types of items. For example, if you have indicated in your policy that users must have either AVG or McAfee as an antivirus, then each host that is assigned this policy is scanned for items in the antivirus category.
Success	Number of successful scans for items within the category.
Failure	Number of failed scans for items within the category.
Totals	Total scans that succeeded, failed and the sum of all scans that were run.

Additional details settings

Field	Definition
General	
Start Time	The start time and date of the report selected when the report was requested.
End Time	The end time and date is set automatically to the time and date that you view the report.
OS list	
OS Details	Total occurrences of the selected scan broken down by operating systems of the hosts that were scanned. This view breaks the list of operating systems down by providing more information about specific service packs or versions.
Category list	
Type	Type of scan engine. Types include: System, Nessus, Admin, and Agent. Agent scans are run using the Persistent Agent, Dissolvable Agent, or the Passive Agent. For information on System, Nessus and Admin Scans see Add a scan on page 616 .
Category	Lists categories included in the selected policy for which the engine is scanning, such as operating system or antivirus. This indicates that there are requirements in the policy for these types of items. For example, if you have indicated in your policy that users must have either AVG or McAfee as an antivirus, then each host that is assigned this policy is scanned for items in the antivirus category.
Name	Name of the specific required item for which the engine is scanning, such as AdAware 2007 or Windows Vista Edition.
Success	Number of successful scans for a specific item within the category.
Failure	Number of times hosts failed the scan for a specific item.
Totals	Total scans for specific items that succeeded, failed and the sum of all scans that were run.

Custom reports

Custom reports allow you to add reports in addition to the standard Templates reports provided.

Reports that you add appear in the drop-down list. You can preview, schedule, modify, and remove the reports. To access Custom Reports select **Logs > Reports**. Select **Custom** from the menu.



Custom reports are stored and displayed for the logged in user. These reports are not globally accessible. Users cannot access other user's custom reports.

Add a custom report

You can add and customize Registrations, Registration Failures, Scan Results, and Connection Logs reports.

1. Select **Logs > Reports**
2. Select **Custom** from the menu.
3. Click **Add**.
4. Select the type of report.

Report Type	Description
Registrations	Successful attempts at registration are displayed based on the selected criteria.
Registration Failures	Failed attempts at registration and login errors are displayed based on the selected criteria.
Scan Results	Scan results are displayed based on the selected criteria. In the Scan Results view or the Health Tab of Host Properties the results display a Passed result for Security/Critical Updates as well as the AutoUpdate. This occurs for all Windows Scans regardless of whether the scan was configured to require the updates. Rogue hosts are not checked unless the scan is configured to require this test. Rogue hosts will otherwise automatically pass the scan.
Connection Logs	Host connections usage information is displayed based on the selected criteria.

5. Enter the name for the report. This name will appear in the drop-down list on the **Custom** tab.



If exporting the report results to .pdf format, do NOT use a colon (:) in the filename.

6. Select the format for the file. For each of the options, the output will be one of the following:
 - HTML
 - CSV
 - EXCEL
 - XML
 - RTF
 - PDF
7. Click **Next** to select the criteria for the report.

Report type	Columns	
Registrations	Address	Location
	City	Operating System
	Description	Phone
	E-mail	Physical Address
	First Name	Sponsor
	Host	State
	ID	Time
	IP address	Title
	Last name	User
Registration Failures		Zip/postal code
	Failure code	Operating system
	Failure description	Physical address
	ID	Time
Scan Results	IP address	
	Host	Scan
	ID	Status
	IP address	Tests
	Location	Time
	Operating system	Type
Connection Logs	Physical address	
	Bytes in	ID
	Bytes out	IP address
	Connect time	Location
	Disconnect time	Physical address

8. Click the item(s) in the list that you want in your report. To move items, use Shift-click to select a range of items or CTRL-click to select individual items.



The items that you select are the column headings on report results.

9. Selected items are highlighted. In the Available Columns panel, click the right arrow to move them to the Selected Columns panel.
10. Click an item in the Selected Columns panel to select it. Use the up and down arrows to rearrange the items in the order that the columns are to appear on the report.



Top to bottom in the list appear left to right in the results.

11. Click **Next**.

12. Enter parameters for the report. These are filters that limit the amount of data returned in the report. Filters are not case sensitive. If you enter smith, the filter returns results for Smith and SMITH.

You can use wildcards when you filter, such as S* in the last name field would return anyone whose last name begins with S. *s* in the last name field would return anyone whose last name contained an s.

13. Click **Finish**. The report is added to the drop-down list on the **Custom** tab.

Parameters

Report type	Parameters	
Registrations	Additional Hardware Information • IP address • Physical Address • Operating system • Location • Description • Host Time (See Calendar Icon on page 801) • Starting • Ending	User Information • ID • Title • Last Name • First Name • Address • City • State • Zip/Postal Code • Phone • E-mail
Registration Failures	User Information • ID Time (See Calendar Icon on page 801) • Starting • Ending	Hardware Information • IP address • Physical address • Operating system
Scan Results	Host Information • ID • IP address • Physical address • Location • Host • Operating system Time (See Calendar Icon on page 801) • Starting • Ending	Scan Details • Status • Type • Scan name
Connection Logs	Host Information • ID • IP address • Physical Address	Device Information • Location Connection Time (See Calendar Icon on page 801)

Report type	Parameters																																																	
Calendar Icon	Time 2009-04-22 00:00:00 2009-05-22 23:59:59   < May 2009 > <table border="1"> <thead> <tr> <th>Su</th> <th>Mo</th> <th>Tu</th> <th>We</th> <th>Th</th> <th>Fr</th> <th>Sa</th> </tr> </thead> <tbody> <tr> <td>26</td> <td>27</td> <td>28</td> <td>29</td> <td>30</td> <td>1</td> <td>2</td> </tr> <tr> <td>3</td> <td>4</td> <td>5</td> <td>6</td> <td>7</td> <td>8</td> <td>9</td> </tr> <tr> <td>10</td> <td>11</td> <td>12</td> <td>13</td> <td>14</td> <td>15</td> <td>16</td> </tr> <tr> <td>17</td> <td>18</td> <td>19</td> <td>20</td> <td>21</td> <td>22</td> <td>23</td> </tr> <tr> <td>24</td> <td>25</td> <td>26</td> <td>27</td> <td>28</td> <td>29</td> <td>30</td> </tr> <tr> <td>31</td> <td>1</td> <td>2</td> <td>3</td> <td>4</td> <td>5</td> <td>6</td> </tr> </tbody> </table>	Su	Mo	Tu	We	Th	Fr	Sa	26	27	28	29	30	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	1	2	3	4	5	6
Su	Mo	Tu	We	Th	Fr	Sa																																												
26	27	28	29	30	1	2																																												
3	4	5	6	7	8	9																																												
10	11	12	13	14	15	16																																												
17	18	19	20	21	22	23																																												
24	25	26	27	28	29	30																																												
31	1	2	3	4	5	6																																												

- Starting
- Ending

Enter the times for Start and End. Format for date and time is YYYY-MM-DD hh:mm:ss

Or use the calendar icon to select the Starting and Ending times for the report.

Time for the selected Start date defaults to 00:00:00.

Time for the selected End date defaults to 23:59:59.

Edit the time parameters to specify a more limited range of data for the generated report.

If you select a start time but no end time, the report is generated with data up to the current time.

If you select an end time, but no start time, the report is generated with all data up to the specified end time.

Preview a custom report

When you have completed adding the Custom report, you can preview the results and export the report to a file for later use. The export formats are HTML, CSV, EXCEL, XML, RTF, and PDF.

1. Select **Logs > Reports**.
2. Select **Custom** from the menu.
3. From the **Custom** tab, select the report name from the drop-down list.
4. Click **Preview**. The report displays in a new browser window.
5. Scroll to the bottom of the report and click an output format.
6. When prompted, click to select **Open** or **Save to Disk**.
7. When selecting Save to Disk, navigate to the appropriate folder, enter a filename, and click **Save**.

Modify a custom report

When you have completed adding and previewing the custom report, you can modify the report to refine the results.

1. Select **Logs > Reports**.
2. Select **Custom** from the menu.
3. From the **Custom** tab, select the report name from the drop-down list.
4. Click **Modify**.

5. The existing type and format information are displayed. Click **Next**.
6. Change the parameters used in the report. See [Add a custom report on page 798](#) for parameters.
7. Click **Next**.
8. Change the information for the report.
9. Click **Finish**. Use the **Preview** function to review the changes.

Remove a custom report

To remove custom reports that are no longer needed:

1. Select **Logs > Reports**.
2. Select **Custom** from the menu.
3. Select the report name from the drop-down list.
4. Click **Remove**.
5. If the report was previously scheduled, select **System > Scheduler** and delete the scheduled report from the list of **Scheduled Tasks**.

Schedule reports

Both the standard report templates and custom reports can be scheduled to run on a regular basis. Custom reports are output to the file format selected by the user when adding the report. The standard reports are output to .pdf files with the filename format `ReportType.MM.DD.YYYY-hh-mm-AM/PM.pdf` with the following filenames:

- PolicyCharts
- PolicyOSReport
- PolicyTestSummary
- RegistrationFailure
- RegistrationOSReport

View scheduled reports by selecting **Logs > Reports > Archives**. The output may be sent to administrators or other users via email. A list of Administrator groups is displayed in the Email group drop-down list in the report schedule view.

Reports via e-mail prerequisites

- The administrators who will receive the email must be members of an Administrator group. This can be the All Management Group or another Administrator group that has been created. See [Groups on page 843](#) for details on creating groups.
- The members of the Administrator group must have an email address in their user record(s) to receive email. See [Add an administrator on page 121](#) for more information.
- The mail server information must also be entered under **System > Settings**. See [Email settings on page 937](#) for more information.

1. Select **Logs > Reports**.
2. **To schedule a standard report:** Go to the **Templates** tab, select a **Report Type** and click **Schedule**.
3. **To schedule a custom report:** Go to the **Custom** tab, select a report and click **Schedule**.

4. Enter a **Name** for the Scheduled task.
5. Select an **Email Group** if you want to share the report.
6. Enter the **Data Range** and select **Days**, **Hours**, or **Weeks** from the drop-down list.
7. Enter the **Schedule Interval** and select **Days**, **Hours**, or **Weeks** from the drop-down list.
8. Enter the **Next Scheduled Time**.
9. Click **Apply**.

Settings

Field	Definition
Name	Name for the scheduled task.
Email Group	Group containing the administrators who will receive the email report results when the scheduled task runs.
Data Range	Number of hours, days, or weeks of data in the report.
Schedule Interval	Length of time the scheduled task waits before running again.
Next Scheduled Time	Initial date/time the task is scheduled to run. Format is MM/DD/YY hh:mm AM/PM.

Archived reports

Archived reports are generated when the scheduled task runs for templates and custom reports.

1. Select **Logs > Reports > Archives**.
2. Click a report in the list to view the contents.
3. Click a heading to sort the reports by **Name** or **Time Generated**.

Scan results

The scan results view displays the results that are maintained in the FortiNAC database of the Dissolvable Agent, the Persistent Agent, and system scans. Access the scan results view from the **Logs** menu.

Settings

Fields used in filters are also defined in this table.

Field	Definition
Scan results	
Time	Time the scan was run.
Scan	Name of the scan used.
User ID	User name of the owner of the host registered in FortiNAC or the MAC address for Rogue hosts.
IP address	IP address of the host at the time it was scanned.
Host	Host name from the Rogue host records or the host name from Registered host records.
Operating System	Operating system on the host.
Location	Name of the switch/port where the host was connected for the scan.
Type	Type of scan performed.
Status	Includes Passed, Failed, Script Failed or Warning.
Right click options	
Export	Exports data to a file in the default downloads location. File types include CSV, Excel, PDF, or RTF. See Export data on page 116 .
Show Details	Displays additional details about the selected scan including: MAC address for all interfaces on the host and the results of any Custom scans associated with the scan used.
Archive & Clear All Scans	Creates an archive of all scans in the database and then removes all scans from the database.
Archive & Clear Selected Scans	Creates an archive of the scans selected in the Scan Results table and then removes those scans from the database.

Show details

The Details window provides information about the scan selected in the Scan Results table. Additional information includes the MAC address for each interface on the host and the results of any custom scans associated with the scan

used to evaluate the host. Scans can have one or more associated custom scans. See [Custom scans on page 560](#).

1. Click **Users & Hosts > Scan Results**.
2. Use the filters to display a list of scans.
3. Select the appropriate scan from the list and click **Show Details**.

Note: Results for Windows Operating System scans can show the following have Passed even when these settings have not been checked in the Scan Configuration:

- Automatic Updates
- Critical Updates
- Internet Connection Sharing
- Security Updates
- Trigger SCCM Evaluation

Archive and clear all scans

Use this option to archive and clear all the Scan Results records. The archived records can be imported later. See [Import archived data on page 102](#) for details.

1. Click **Users & Hosts > Scan Results**.
2. Click **Archive & Clear All Scans**.
3. Click **Yes** on the confirmation window.
4. All the records are archived in a file using the following name format: RESULTS_Archive_YY_MM_DD:hh:mm:ss.bua.gz

Archive and clear selected scans

Use this option to archive and clear the selected Scan Results records. You can import archived records at another time. See [Import archived data on page 102](#) for details.

1. Click **Users & Hosts > Scan Results**.
2. Use the filters to display a list of scans.
3. Click a record to select it. Use either Shift-click or Ctrl-click to select additional records.
4. When you have selected the records, click **Archive & Clear Selected Scans**.
5. Click **Yes** on the confirmation window.
6. The selected records are archived in a file with the following name format: RESULTS_Archive_YY_MM_DD:hh:mm:ss.bua.gz

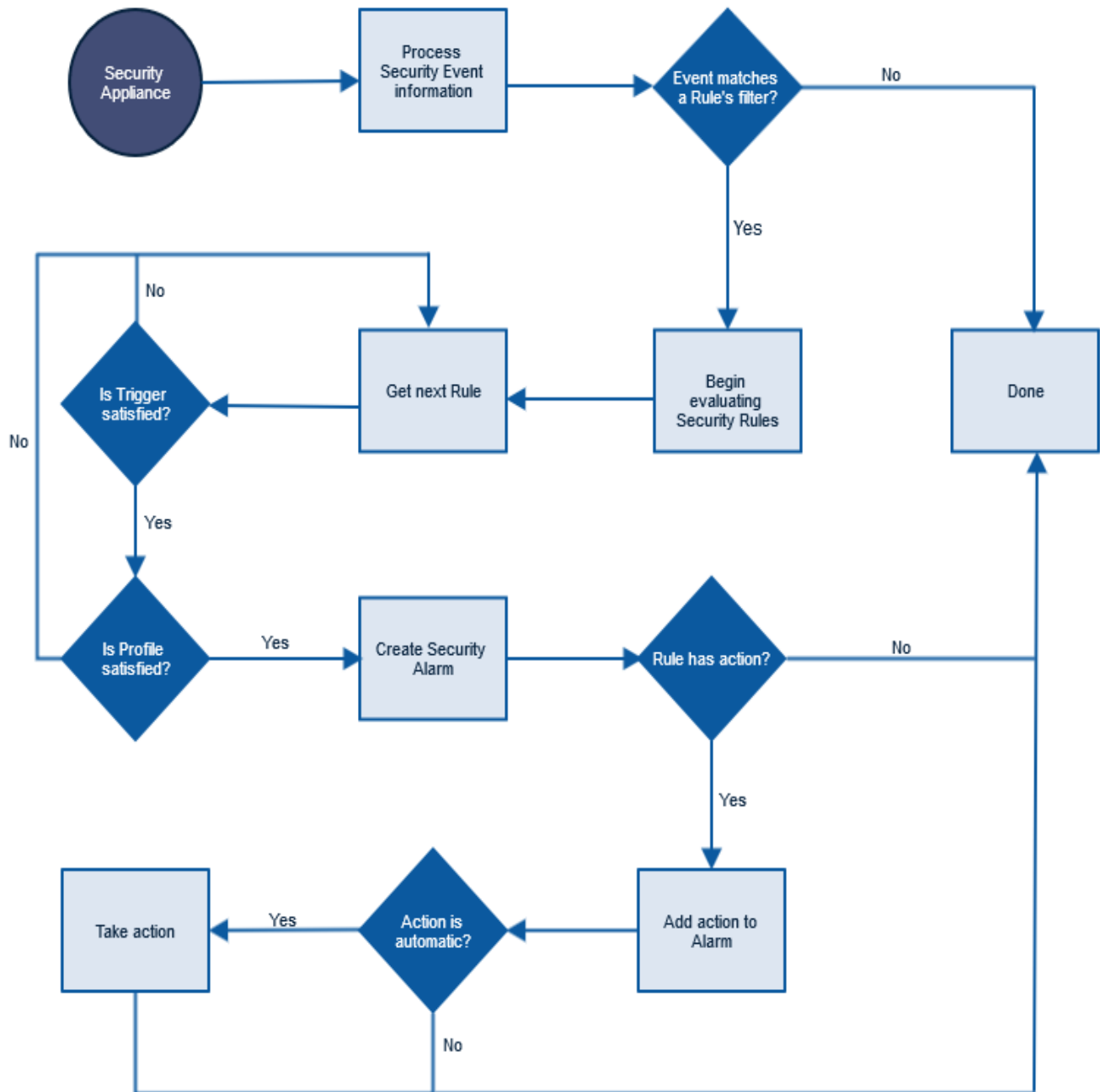
Security Incidents

Security Incidents integrates with security solutions such as FireEye, Fortinet, and Palo Alto Networks to correlate security alerts. Incoming information is normalized into a consistent security event format and provide additional information about the source hosts.

Security Incidents isolates restricts, or blocks compromised endpoints and reduces threat containment time by:

- Automating actions on an event based on policies.
- Providing information in security alerts.
- Prioritizing security events.
- Tracing a threat across IT domains and automating an action to minimize the threat containment time.

If you have not purchased the Security Incidents license you will not be able to access the Security Incidents features.



Implementation

Security Incidents allows you to build Security Rules to trigger on administrator defined-patterns of Security Events to generate Security Alarms. Security Rules can be targeted to only generate alarms for specific hosts, users, and locations. Actions can be taken on Security Alarms to isolate or block compromised hosts automatically.

This section of the documentation discusses the implementation in the order in which it should be done. As the options are discussed, links to additional information are provided.

Network devices

Find or create devices

You will need to find or create the network devices you wish to configure. See [Find containers or devices on page 41](#) or [Add or modify a pingable device on page 302](#). For pingable devices, Security Incidents provides the Security Events option. This allows you to select a security appliance from which events may be accepted in order to create a security event when an event rule is matched.

Threat analysis engines

When you have configured the security devices, you can create threat analysis engines, which will scan applications on the host to determine the threat level, and provide a threat score.

Security policies

Security rules

Once you have configured your network devices, you must create security rules. Security Rules contain triggers that correlate incoming events from the network devices and create an alarm. Defined in the host profile, security rules determine which actions to take based on the alarm that is triggered by the host. See [Rules on page 817](#).

Creating a security rule to catch all incoming events enables you to analyze traffic and identify patterns in order to create rules based on this information. Add a trigger with a single filter, with a minimum severity of 0 and a maximum severity of 10. This will ensure that incoming events of all severity levels are captured by the system.

After you create the trigger, add a security rule using the trigger and set both the user/host profile and Action to None.



This Security Rule will catch all incoming events. To ensure that it does not interfere with normal system operation, it should be the lowest ranked rule.



Because this Security Rule will produce a large number of security events, it will affect system performance. The Security Rule should only be enabled in production during specific times, such as off hours.

Once all incoming Security Events are captured, you can create Security Rules directly from the Security Events view based on various types of Security Events.

Permissions

You must provide permissions for users to view security alarms that are created when a security rule is matched. Users can may then take action on a security alarm if it was not done automatically. You can allow the user to take any action on an alarm, or specify the actions the user is allowed to take. See [Add an administrator profile on page 139](#).

Monitor the system

You can monitor and take actions on alarms created from incoming events that satisfy triggers established by security rules that are defined for the host. See [Events on page 814](#).

A security rule with a trigger satisfied and a matching User/Host profile creates a security alarm. The rule may then take an action automatically. The action for a higher-ranked rule takes precedence over the action for a lower-ranked rule. The lower-ranked rule is not implemented automatically, but can still be done manually. However, the action for a higher-ranked security rule will override a lower-ranked rule that was previously implemented.

You can configure the application settings when creating the security rule in Policy Configuration. See [Add or modify a rule on page 819](#). As hosts are scanned by the agent, the applications are updated. The security rule includes the applications as part of the trigger that will create an alarm when the rule is satisfied. See [Application view on page 243](#).

Security event severity level mappings

Each vendor defines its own severity levels for syslog messages. These severity levels are normalized within FortiNAC to provide additional filtering options for incoming security events. The following table provides severity level mappings between the vendor and FortiNAC.

CheckPoint

Vendor severity level	FortiNAC severity level
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
10	10

Stonegate

Vendor severity level	FortiNAC severity level
0	1
1	2
2	3

Vendor severity level	FortiNAC severity level
3	4
4	5
5	6
6	7
7	8
8	9
9	10

TippingPoint SMS

Vendor severity level	FortiNAC severity level
0	1
1	3
2	5
3	7
4	9

FireEye

Vendor severity level	FortiNAC severity level
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8
8	9
9	10

FortiOS

Vendor severity level	FortiNAC severity level
INFORMATION	1
NOTICE	3
WARNING	5
ALERT	7
CRITICAL	8
ERROR	9
EMERGENCY	10

PaloAlto

Vendor severity level	FortiNAC severity level
INFORMATIONAL	1
LOW	3
MEDIUM	5
HIGH	7
CRITICAL	9

Vendor severity levels

Each vendor defines its own severity levels for syslog messages. The following table shows the equivalent FortiNAC security level.

Vendor	Vendor severity level	FortiNAC severity level
CheckPoint	1	1
	2	2
	3	3
	4	4
	5	5
	6	6
	7	7
	8	8
	9	9
	10	10
FireEye	0	1
	1	2
	2	3
	3	4
	4	5
	5	6
	6	7
	7	8
	8	9
	9	10
Fortinet	INFORMATION	1
	NOTICE	3
	WARNING	5
	ALERT	7
	CRITICAL	8
	ERROR	9
	EMERGENCY	10

Vendor	Vendor severity level	FortiNAC severity level
PaloAlto	INFORMATIONAL	1
	LOW	3
	MEDIUM	5
	HIGH	7
	CRITICAL	9
RSA	0	1
	1	2
	2	3
	3	4
	4	5
	5	6
	6	7
	7	8
	8	9
	9	10
Stonegate	0	1
	1	2
	2	3
	3	4
	4	5
	5	6
	6	7
	7	8
	8	9
	9	10
TippingPointSMS	0	1
	1	3
	2	5
	3	7
	4	9

Events

Security events displays all incoming security events to FortiNAC that satisfy a security trigger. FortiNAC automatically reviews all security rules for each event. When an event satisfies a trigger associated with a rule, an alarm is created.

You can also create an event rule based on one or more security events in the list.

To view security events, go to **Logs > Security Incidents > Events**.

Settings

The fields listed in the table below are displayed in columns on the **Security Events** view based on the selections you make in the **Settings** window.

Field	Definition
Add Filter	Allows you to select a field from the current view to filter information. Select the field from the drop-down list, and then enter the information you wish to filter. See Filters on page 34 .
Update	Displays the filtered data in the table.
Pause	Allows user to pause the Security Event view from updating with new events so specific events can be viewed more easily.
Events	
Event Date	The date when the event was received.
Source IP	The IP address for the host that triggered the event.
Source MAC	The MAC address of the host that triggered the event.
Destination IP	The IP address of the host or device the source host was communicating with.
Alert Type	The type of security event was received.
Subtype	The subtype of the security event.
Severity	The severity of the event reported by the security appliance.
Threat ID	A unique identifying code supplied by the vendor for the specific type of threat or event that occurred.
Event Description	A description supplied by the security appliance of the event.
Location	The location of the source host is on the network. For example, this could be the SSID the host is connected to wirelessly, or the port the host is plugged into on a switch.
Buttons	
Export	Use the Export option to export a list of selected hosts to CSV, Excel, PDF, or RTF formats.
Options	Options displays the same series of menu picks displayed when the right-mouse button is clicked on a selected alarm.
View Details	Displays the details of the security event.

Field	Definition
View Host	Opens the Modify Host window to view and update the details of the host associated with the selected security event.
Right click options	
View Details	Displays the details of the security event.
View Host	Opens the Modify Host window to view and update the details of the host associated with the selected security event.
View in Host View	Opens the host in Host View.
Create Event Rule	Allows user to create a rule based on the selected events.

Add an event rule from security events

You can create security event rules directly from the **Security Event** view. This enables you to create security rules directly from security events as the events occur.

1. Click **Logs > Security Incidents > Events**.
2. Use the filters to locate the appropriate event.
3. Select the event(s) you wish to use to create the rule. You can select multiple events at a time.
4. Right-click and select **Create Event Rule**.
5. Select the field(s) from the **Available Fields** column, and then click the right-arrow to add the fields to the **Selected Fields** column.
6. Click **OK**.
7. The Add Security Trigger window appears. The selected fields populate the trigger filter fields.
8. Add the details of the trigger. See .
9. Click **OK**.
10. The Add Security Rule window appears.
11. Add the details of the security rule. See .

The security rule is added to the list of rules in the **Security Rules** view.

Alarms

FortiNAC generates a security alarm when a security rule runs.

When you click a specific alarm, the details of the event(s) that triggered the alarm appear in the **Events** tab. You can also create a new event rule based on the events in the list. The **Actions Taken** tab displays the actions that were taken for the alarm, the completion status, and whether they were successfully (if applicable).

The fields listed in the table below are displayed in columns on the **Security Alarms** view based on the selections you make in the **Settings** window.

Field	Definition
Add Filter	Allows you to select a field from the current view to filter information. Select the field from the drop-down list, and then enter the information you wish to filter. See Filters on page 34 .
Update	Displays the filtered data in the table.
Pause	Allows user to pause the Security Alarms view from updating with new alarms so specific alarms can be viewed more easily.
Security alarms	
Host MAC	The MAC address for the host that triggered the alarm. Click the MAC address to open the Modify Host window where you can register the host and modify host details. See Add or modify a host on page 227 .
Alarm Date	The date when the alarm was created.
Matched Rule	The name of the rule that created the alarm.
Action	The associated action from the rule when the alarm was created or the action was taken on the alarm. Users can click the action to open the Modify Security Action window and modify the action. See . If an action is associated to an alarm but was not taken, and the action is then deleted from the Security Actions view, the action is disassociated from the alarm and users may take a new action on the alarm. If an action was taken on an alarm, and the action is then deleted from the Security Actions view, the action remains visible but is not editable.
Action Taken Date	If an action was taken, shows the date when the action was taken.
Action Taken By	The user who manually took the action on the alarm.
Action Undone Date	If the action was undone, shows the date when the action was undone.
Action Undone By	The user who manually undid the action.
Buttons	
Export	Use the Export option to export a list of selected hosts to CSV, Excel, PDF, or RTF formats.
Options	Options displays the same series of menu picks displayed when the right-mouse button is clicked on a selected alarm.
Take Action	User can manually take action on the selected alarm, if action has not already been taken.
Undo Action	User can undo an action if the action has been taken on the selected alarm, but has not been undone.
View Host	Opens the Modify Host window to view and update the details of the host that triggered the alarm. See Add or modify a host on page 227 .
Right click options	

Field	Definition
Take Action	User can manually take action on the selected alarm, if action has not already been taken.
Undo Action	User can undo an action if the action has been taken on the selected alarm. When the action is undone, the secondary task is performed on the host if enabled.
View Host	Opens the Modify Host window to view and update the details of the host associated with the selected security event. See Add or modify a host on page 227 .
View in Host View	Opens the host in Host View. See Hosts on page 213 .
Events tab	
Event Date	The date when the event that triggered the alarm occurred.
Source IP	The IP address for the host that triggered the event.
Source MAC	The MAC address of the host that triggered the event.
Destination IP	The IP address of the host or device the source host was communicating with.
Alert Type	The type of security event that triggered the alarm.
Subtype	The subtype of the security event.
Severity	The severity of the event reported by the security appliance.
Threat ID	A unique identifying code supplied by the vendor for the specific type of threat or event that occurred.
Event Description	A description supplied by the security appliance of the event.
Location	The location of the source host is on the network. For example, this could be the SSID the host is connected to wirelessly, or the port the host is plugged into on a switch.
Right click options	
View Details	Displays the details of the security event that triggered the alarm.
View Host	Opens the Modify Host window to view and update the details of the host associated with the selected security event. See Add or modify a host on page 227 .
View in Host View	Opens the host in Host View. See Hosts on page 213 .
Create Event Rule	Allows user to create a rule based on the selected events.
Actions taken tab	
Action	The action that was taken on the alarm.
Completed	Indicates whether the action was completed.

Rules

Create and manage security rules based on triggers that correlate incoming events from network devices. When a security event is received, the highest ranked security rule with a trigger satisfied and a matching User/Host profile creates a security alarm. The rule may then take an action automatically.

Settings

An empty field in a column indicates that the option has not been set.

Field	Definition
Rank	Moves the selected rule up or down in the list. Incoming events are compared to rules in order by rank.
Set Rank	Allows you to type a different rank number for a selected rules and immediately move the rule to that position. In an environment with a large number of rules this process is faster than using the up and down buttons.
Table columns	
Rank	Rule's rank in the list of rules. Rank controls the order in which incoming events are compared to Security Rules.
Name	User defined name for the security rule.
Enabled	Indicates whether the rule has been enabled.
Trigger	The set of events that will activate the rule if the rule is enabled.
Host Profile	The host profile to which the security rule applies. The = sign indicates the host must match the user host profile. The ≠ indicates the host must not match the user host profile. An alarm is triggered when the security rule is satisfied.
Action	The action that will be associated or automatically taken when the security rule is activated.
Rule Match Email Group	If enabled in the security rule, the administrator group that will receive an email when the rule creates an alarm.
Action Taken Email Group	If enabled in the security rule, the administrator group that will receive an email when an action is taken on the created alarm.
Last Modified By	User name of the last user to modify the security rule.
Last Modified Date	Date and time of the last modification to this security rule.
Right click options	
Delete	Deletes the selected security rule.
Modify	Opens the Modify Security Rule window for the selected security rule.
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746 .
 You must have permission to view the admin auditing log. See Add an administrator profile on page 139.	

Add or modify a rule

1. Select **Logs > Security Incidents > Rules**
2. Click **Add** or select an existing security rule and click **Modify**.
3. Click in the **Name** field and enter a name for this security rule.
4. Use the table below to enter the security rule information.
5. Click **OK** to save your security rule.

Settings

Field	Definition
Rule Enabled	Select this check box to activate the security rule.
Name	A unique name for this security rule.
Trigger	The trigger that will activate the rule. You can use the icons next to the Trigger field to add a new trigger or modify the trigger shown in the drop-down menu. When you modify this trigger, it is modified for all security rules that make use of the trigger.
User/Host Profile	Indicates whether the rule must match or not match the host profile selected from the drop-down menu. You can use the icons next to the Host Profile field to add a new host profile or modify the profile shown in the drop-down menu. A host profile is not applied to the trigger when None is selected.
Action	The action assigned to the security rule. You can select whether the action should be manual or automatic. You can use the icons next to the Action field to add a new action or modify the action shown in the drop-down menu. Note that by selecting None , an action is not assigned to the trigger.
Send Email when Rule is Matched	Select this check box to automatically send an email to the selected administrator group when the security rule creates an alarm.
Admin Group drop-down menu	Select the administrator group list that will receive the email when an alarm is created.
Send Email when Action is Taken	Select this check box to automatically send an email to the selected administrator group when the action associated with the security rule is taken.
Admin Group drop-down menu	Select the administrator group to be notified when the action associated with the security rule is taken.
Admin Group Email Content	When you select Send Email when Rule is Matched and/or Send Email when Action is Taken, the email message that is sent to the selected Admin group contains information such as the security rule that was matched, the date and time of the alarm, the host and MAC address information, severity, and location of the host. The following is an example of the content included in the email: Security Rule Matched = PA_test Alarm Date/Time = 2015-09-28 17:04:36.0 User ID = testuser No owner Host Name = testuser-PC Host OS = Windows 7 Professional 6.1 Service Pack 1

Field	Definition
	Host Hardware = Host MAC addresses = 5C:26:0A:44:53:1D,00:24:D7:A2:24:5C,00:50:56:C0:00:01,00:50:56:C0:00:08 Host IP addresses = 192.168.10.139,192.168.4.169,192.168.204.1,192.168.74.1 Host Locations = Concord-3750 Fa3/0/6,Concord_Cisco_1131.example.com VLAN 4 Date = 2015-09-28 17:04:35.0 Alert Type = THREAT Severity = null ThreatID = null Description = HTTP OPTIONS Method(30520) Source IP = 192.168.10.139 Source MAC = 5C:26:0A:44:53:1D Destination IP = 23.96.61.106 Location = Concord-3750 Fa3/0/6 Vendor = PaloAlto

Delete a rule

1. Select **Logs > Security Incidents > Rules**
2. Select a rule and click **Delete**.
3. A confirmation message is displayed. Click **Yes** to continue.

Triggers

Create triggers for security rules to correlate incoming security events from network devices. When an incoming security event satisfies a trigger, all security rules using the trigger are evaluated in order of their rank. A security alarm is created based on the first security rule which also matches its optional user/host profile. If no security rules are matched, an alarm is not created. An optional security action will be associated to the alarm and, if selected, will be executed automatically.

Settings

Field	Definition
Add Filter	Allows you to select a field from the current view to filter information. Select the field from the drop-down list, and then enter the information you wish to filter.
Update	Displays the filtered data in the table.
Table columns	
Name	User defined name for the trigger. The type of event that will activate the rule if the rule is enabled.
Time Limit	The time span to satisfy all required filters for the trigger to be satisfied.
Filter Match	The number of filters that must be matched by security events for the trigger to be satisfied. Select Any to set the minimum number of filters that must be matched. Select All to specify that all filters must be matched.

Field	Definition
Total Filters	The number of security filters associated with the security trigger.
Last Modified By	User name of the last user to modify the security trigger.
Last Modified Date	Date and time of the last modification to this security trigger.
Right click options	
Delete	Deletes the selected trigger.
Modify	Opens the Modify Security Trigger window for the selected trigger.
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746 .
 You must have permission to view the admin auditing log. See Add an administrator profile on page 139 .	

Add a trigger

To verify that events are being captured, create a catch all rule to log the security events.

1. Select **Logs > Security Incidents > Triggers**
2. Click **Add** or select an existing security trigger and click **Modify**.
3. Click in the **Name** field and enter a name for this security trigger.
4. Use the table below to enter the security trigger information.
5. Click **OK** to save your security rule trigger.

Settings

Field	Definition
Name	A name for this security trigger.
Time Limit	The amount of time within which the incoming events must occur before satisfying the trigger.
Filter Match	Select whether any size subset of the security filters must be matched in order to satisfy the trigger.
Not currently in use/In use by	Indicates whether the trigger is in use, and the number of rules currently associated with the trigger.
Security filters	
Frequency	The number of times the security event must occur from the vendor in order to satisfy the trigger.
Vendor	The name of the vendor that is sending the security event.
Type	Specifies the type of security event.

Field	Definition
Sub Type	Specifies the subtype of security event.
Threat ID	A unique identifying code supplied by the vendor for the specific type of threat or event that occurred.
Description	A textual description supplied by the security appliance of the event.
Severity	The range within which the threat level must be defined in order to satisfy the trigger.
Number of Custom Fields	The number of custom fields that were added to the filter.
Add	Click to add a filter.
Modify	Click to modify a selected filter.
Delete	Click to delete a selected filter.
Not currently in use/In use by	Indicates whether the action is in use, and the number of rules currently associated with the action.

Delete a trigger

1. Select **Logs > Security Incidents > Triggers**
2. Select a trigger and click **Delete**.
3. A confirmation message is displayed. Click **Yes** to continue.

Add or modify filters

1. Navigate to **Logs > Security Incidents > Triggers**
2. Click **Add** or select a security trigger and click **Modify**.
3. Under **Security Filters**, click **Add**, or select a filter and click **Modify**.
4. Use the table below to enter the security filter information.
5. Click **OK** to save your security filter.

Settings

Field	Definition
Frequency	The number of times the security event must occur from the vendor in order to satisfy the trigger.
Vendor	The name of the vendor that is sending the security event.
Type	Specifies the type of security event.
Sub Type	Specifies the subtype of security event.
Threat ID	The code generated by the vendor for the security event threat level.
Description	Additional details about the security event.

Field	Definition
Severity Range	The range within which the threat level must be defined in order to satisfy the trigger.
Custom Fields	The custom fields that were added to the filter. Click Add to add a custom field. Click Modify to modify a selected field. Click Delete to delete a selected field.

Delete a filter

1. Select **Logs > Security Incidents > Triggers**
2. Select a trigger and click **Modify**.
3. Select a security filter and click **Delete**. The filter is deleted.
4. Click **OK**.

Actions

The **Actions** view allows you to add, modify, and delete actions that can be associated to an alarm. If the action is selected, it can be executed automatically or manually, depending on the security rule configuration.

Settings

Field	Definition
Add Filter	Allows you to select a field from the current view to filter information. Select the field from the drop-down list, and then enter the information you wish to filter. See Filters on page 34 .
Update	Displays the filtered data in the table.
Table columns	
Name	User defined name for the action. The type of action that will occur if the rule is enabled.
Activity Failure	Indicates whether the system will continue to perform activities for the action if a higher-ranked activity fails. When Continue Running Activities is selected, the next ranked activity in the list is performed after a higher-ranked activity fails. When Stop Running Activities is selected, no lower-ranked activities are executed when a higher-ranked activity fails.
Secondary Task Delay	The amount of time that will pass before the enabled secondary activity is executed for an activity. For example, the user may wish to enable the host 15 minutes after the host was initially disabled.
Activity Summary	A description of the activity that will occur.
Last Modified By	User name of the last user to modify the action.
Last Modified Date	Date and time of the last modification to this action.
Right click options	
Delete	Deletes the selected action.

Field	Definition
Modify	Opens the Modify Security Action window for the selected action.
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746 .
 You must have permission to view the admin auditing log. See Add an administrator profile on page 139 .	

Add or modify an action

1. Go to **Logs > Security Incidents > Actions**
2. Click **Add** or select an existing security action and click **Modify**.
3. Click in the **Name** field and enter a name for this security action.
4. Use the table below to enter the security action information.
5. Click **OK** to save your security rule action.

Settings

Field	Definition
Name	A name for this security action.
On Activity Failure	User indicates whether the system will continue to perform activities for the action if a higher- ranked activity fails. When Continue Running Activities is selected, the next ranked activity in the list is performed after a higher-ranked activity fails. When Stop Running Activities is selected, no lower-ranked activities are executed when a higher-ranked activity fails.
Perform Secondary Tasks After check box	When selected, if a secondary task is enabled for an activity, the secondary task is automatically executed to undo the action. The user may enter the amount of time that will pass between the primary and secondary tasks. If the check box is not selected, the user may manually undo the action in the Security Alarms view.
Not currently in use/In use by	Indicates whether the action is in use, and the number of rules currently associated with the action.
Activities	
Rank Buttons	Moves the selected action up or down in the list. Activities are performed in order by rank.
Rank	The activity's rank in the list of activities. Rank controls the order in which activities are performed.
Activity	Specifies the activity that will be performed.

Field	Definition
Add	Click to add an activity.
Modify	Click to modify a selected activity.
Delete	Click to delete a selected activity.

Delete an action

1. Select **Logs > Security Incidents > Actions**
2. Select an action and click **Delete**.
3. A confirmation message is displayed. Click **Yes** to continue.

Add or modify activities

1. Select **Logs > Security Incidents > Actions**
2. Click **Add** or select an action and click **Modify**.
3. Under **Activities**, click **Add**, or select an activity and click **Modify**.
4. Select the activity from the **Activity** drop-down menu.
5. Enter the information associated with the activity.
6. Some options include the **Secondary Task** check box. Selecting this check box enables the secondary task to occur after the time period specified in the action has passed.
7. Use the table below for information about each activity option.
8. Click **OK** to save your activity.

Settings

Field	Definition
Command Line Script Action	Lets you specify a particular command line script to be executed as an alarm action.
Send Alarm to Custom Script	Lets you send an alarm to a custom command line script located in /home/cm/scripts when the trigger event occurs.
Send Alarm to External Log Hosts	Sends an alarm to an external log host when the trigger event occurs.
Email User Action	Sends an email to the logged on user or owner, only the logged on user, or only the owner when the action is taken. See Hosts on page 213 for more information about adding or modifying the host's owner. Enter the message for the user in the Email Message box. Select the fields to display information you wish to append to the email. You can update the text to be displayed for each field.

Field	Definition
	Users can add or modify custom fields that are appended to the email. Custom fields include information about a security event that is stored under Full Event Attributes in the Security Events View > Event Details window. For example, enter a label for the field and the "CS4" key to display the CS4 information in the custom field. See Events on page 814
Email Group Action	Sends an email to the selected administrator group.
SMS User Action	Sends an SMS message to the host's owner when the action is taken. See Hosts on page 213 for more information about adding or modifying the host's owner. Enter the message for the user in the SMS Message box.
Host Role Action	Lets you set the host role to any configured role. You can select the Secondary Task check box to enable a secondary task to change the role when the action is undone.
Disable Host	Disconnects the host from the network. You can select the Secondary Task check box to enable the host after a specified time period if the Perform Secondary Task(s) check box is enabled for the action.
Disable Port	Disconnects the port. You can select the Secondary Task check box to enable the port after a specified time period if the Perform Secondary Task(s) check box is enabled for the action.
Run Endpoint Compliance Configuration	When selected, allows you to run additional endpoint compliance configurations based on security actions mapped to a scan's results. See Chaining configuration scans on page 540 .
Mark Host At Risk	Automatically fails the scan selected in the Mark Host At Risk For drop-down list, and places the host in a state of remediation the next time the host connects. You can select the Secondary Task check box to mark the host safe after a specified time period if the Perform Secondary Task(s) check box is enabled for the action.
Mark Host Safe	Automatically marks the host as safe for the scan selected in the Mark Host Safe For drop-down list, and passes the scan. You can select the Secondary Task check box to mark the host at risk after a specified time period if the Perform Secondary Task(s) check box is enabled for the action.
Send Message to Desktop	Lets you send a message to the desktop of a host running the Persistent Agent.

Delete an activity

1. Go to **Logs > Security Incidents > Actions**
2. Select an action and click **Modify**.
3. Select an activity and click **Delete**. The activity is deleted.
4. Click **OK**.

System

Certificate management	828
Config wizard	839
Cluster Management	839
Groups	843
Feature Visibility	856
Scheduler	857
Tasks	862
Settings	863
Roaming guests	901
Multi-factor Authentication	903
Reports	932
Custom Health Check	976

Certificate management

This section covers certificate management.

- [Server certificates on page 828](#)
- [Trusted certificates on page 835](#)

Server certificates

This view allows the administrator to install SSL server certificates in order to encrypt connections with FortiNAC. Different features in FortiNAC require certificates. The Certificate Target is used to specify the feature to which the certificate will be applied. See **Certificate Target** in the Settings table below for more details.

NOTE: Installing certificates under the Server Certificates tab does not automatically add the root/intermediate certificate to the corresponding target under the Trusted Certificates tab.

Example:

Server Certificates tab Certificate Target: "Local RADIUS Server (RadSec)"

Corresponding Trusted Certificates tab Target "RADIUS Endpoint Trust (RadSec)"

Settings

Field	Definition						
Add Filter	Allows you to select a field from the current view to filter information. Select the field from the drop-down list, and then enter the information you wish to filter. See Filters on page 34 .						
Update	Displays the filtered data in the table.						
Certificate Target	The component where the certificate is applied. <table><tr><th>Target</th><th>Description</th></tr><tr><td>Admin UI</td><td>Used to secure connections with the Administration UI. Note some browsers require certificates (other than the default self-signed certificate) in order to allow data to be exported from the UI. Exportable data examples include Endpoint Compliance, User Accounts, Hosts and Adapters.</td></tr><tr><td>New Remote API Target</td><td>Used for installing certificates for a custom alias (such as Microsoft InTune MDM). Example: Remote API[msintune]</td></tr></table>	Target	Description	Admin UI	Used to secure connections with the Administration UI. Note some browsers require certificates (other than the default self-signed certificate) in order to allow data to be exported from the UI. Exportable data examples include Endpoint Compliance, User Accounts, Hosts and Adapters.	New Remote API Target	Used for installing certificates for a custom alias (such as Microsoft InTune MDM). Example: Remote API[msintune]
Target	Description						
Admin UI	Used to secure connections with the Administration UI. Note some browsers require certificates (other than the default self-signed certificate) in order to allow data to be exported from the UI. Exportable data examples include Endpoint Compliance, User Accounts, Hosts and Adapters.						
New Remote API Target	Used for installing certificates for a custom alias (such as Microsoft InTune MDM). Example: Remote API[msintune]						

Field	Definition												
	<table> <tr> <th>Target</th><th>Description</th></tr> <tr> <td>New SAML Target (F 7.6.3 +)</td><td>Used to secure connections between FortiNAC and external Identity Provider (IdP) for Admin SAML SSO integration. See SAML SSO integration guide for details. https://docs.fortinet.com/document/fortinac-f/7.6.3/saml-ss/</td></tr> <tr> <td>Portal</td><td>Used to secure connections involving the Dissolvable Agent or captive portal. See Portal SSL for details.</td></tr> <tr> <td>Persistent Agent</td><td>Used to secure connections between FortiNAC and Persistent Agents.</td></tr> <tr> <td>New Local RADIUS Server Target (EAP)</td><td>Used to secure the connection for a RADIUS server when multiple Local RADIUS server configurations are required. See Virtual Servers.</td></tr> <tr> <td>Remote API [remote_api]</td><td>Used for installing certificates for (such as for Microsoft InTune MDM). This is the default api target with a pre-defined alias of "remote_api." The alias cannot be changed.</td></tr> </table>	Target	Description	New SAML Target (F 7.6.3 +)	Used to secure connections between FortiNAC and external Identity Provider (IdP) for Admin SAML SSO integration. See SAML SSO integration guide for details. https://docs.fortinet.com/document/fortinac-f/7.6.3/saml-ss/	Portal	Used to secure connections involving the Dissolvable Agent or captive portal. See Portal SSL for details.	Persistent Agent	Used to secure connections between FortiNAC and Persistent Agents.	New Local RADIUS Server Target (EAP)	Used to secure the connection for a RADIUS server when multiple Local RADIUS server configurations are required. See Virtual Servers .	Remote API [remote_api]	Used for installing certificates for (such as for Microsoft InTune MDM). This is the default api target with a pre-defined alias of "remote_api." The alias cannot be changed.
Target	Description												
New SAML Target (F 7.6.3 +)	Used to secure connections between FortiNAC and external Identity Provider (IdP) for Admin SAML SSO integration. See SAML SSO integration guide for details. https://docs.fortinet.com/document/fortinac-f/7.6.3/saml-ss/												
Portal	Used to secure connections involving the Dissolvable Agent or captive portal. See Portal SSL for details.												
Persistent Agent	Used to secure connections between FortiNAC and Persistent Agents.												
New Local RADIUS Server Target (EAP)	Used to secure the connection for a RADIUS server when multiple Local RADIUS server configurations are required. See Virtual Servers .												
Remote API [remote_api]	Used for installing certificates for (such as for Microsoft InTune MDM). This is the default api target with a pre-defined alias of "remote_api." The alias cannot be changed.												
Applied to	This column only shows if the appliance is in a 1+1 or N+1 HA group and is currently in control. It shows if the certificate is applied to the primary server or the secondary server *when it's in control*. Can only have two values: Primary or Secondary.												
Alias	Indicates how the certificate is stored in the underlying Keystore.												
Issued To	The server that received the certificate. Displays information entered when generating the CSR.												
Issued By	The CA that issued the certificate.												
Expiration	The date when the certificate expires and a new certificate is required. Users can map events to alarms when the certificate will expire or has expired. See Map events to alarms on page 784 .												
Buttons													
Generate CSR	Opens the Generate CSR window to enter the CSR details.												
Upload Certificate	Opens the Upload Certificate window to find and select the key and certificate. For the PKCS#12 certificate option, upload the .pfx or .p12 file with the public key certificate and the corresponding private key bundle, and enter the password of the PKCS#12 certificate file. High Availability Note: The UI does not have the option to install certificates on both the primary and secondary servers at the same time. Certificates uploaded using this view apply to the server currently in control.												
Details	Opens the details and private key information for the selected target.												
Copy Certificate	Opens the copy certificate window to copy a certificate from a Certificate Target source to a Certificate Target destination.												

Field	Definition
Restart Service	Opens the restart service window to restart the selected Certificate Target.
Download	Download the selected certificate file in the file name of "certificate.cert". By default, the file will be downloaded to the local host or machine. (Only PEM format is supported. PKCS#12 format is available to download via CLI, please see Download a certificate on page 833)
Export	Exports to a CSV, Excel or RTF file the following information displayed in the current Certificate Management view (Server Certificates or Trusted certificates): Server Certificates Details Certificate Target Alias Issued to Issued by Expiration Note: This function does not export the certificate files.

High Availability(HA) Certificate Management

Starting in version 7.6.5, FortiNAC introduces a redesigned High Availability (HA) certificate management system that simplifies how certificates are handled between the primary and secondary servers in both 1+1 and N+1 HA configurations.

Administrators can now generate, upload, or copy certificates for the secondary server directly from the primary server's GUI. Likewise, if the secondary server is in control during a failover, it can manage certificates for the primary. All configured certificates are automatically synchronized between servers to ensure continuity.

For more information on High Availability, see the [1+1 HA documentation](#) and the [N+1 HA documentation](#).

Key Changes in the new HA System

- The primary and secondary servers can share the same certificate alias name, allowing for consistent configuration references (for example, "common_radius").
- Even though the alias name can be the same, the actual certificates must be different, each with its own unique Common Name (CN).
- This design ensures a smooth and automatic transition during failover without conflicts or manual reconfiguration.
- Certificates are synchronized between servers but remain specific to their assigned role (primary or secondary).

Understanding the "Applied To" Field

The Applied To column in the **Certificate Management** page indicates which server a certificate is intended for:

- **Primary** – The certificate is used by the primary server in normal operation.
- **Secondary** – The certificate is used by the secondary server when it becomes active (for example, during a failover).

This field helps administrators quickly identify which certificate belongs to which server, even if both use the same alias.

Additional Notes

- The **Certificate Management** page is visible on the secondary server only when it is in control.
- Each certificate can only be used by one server at a time. If the same certificate needs to be used on both servers, it must be copied from one to the other.
- In N+1 configurations, multiple primary servers can each synchronize their own certificates (with the same alias but different CNs) to a shared secondary server.

Obtain a certificate from CA

If you do not already have a certificate, you must obtain a certificate from a Certificate Authority (CA). FortiNAC does not have the ability to issue certificates.

To obtain a valid third party SSL certificate from a CA, you must generate a CSR and send it to the CA.

1. Go to **System > Certificate Management**
2. Click **Generate CSR**.
3. (If this appliance is in a HA group) Select the server to which the certificate will be applied.
4. Select the certificate target to which the certificate will be applied.
5. Enter the **Common Name**. This is the hostname to be secured by the certificate. If generating a wildcard CSR, enter the desired domain specifying the wildcard in the **Common Name** field (Example: *.example.com).
6. Enter the Subject Alternative Names (leave blank if not requesting a SAN certificate). Click **Add** to enter each additional hostname and/or IP address.
7. Enter the **Key and Signature Algorithm**.

RSA

RSA is a widely used asymmetric encryption algorithm based on the difficulty of factoring large numbers. It employs a pair of keys: the public key for encryption and the private key for decryption. The public key can be openly distributed, while the private key must be kept strictly confidential. The security of RSA relies on the difficulty of factoring the product of two large prime numbers.

ECDSA (Version F 7.6.5+)

After Version F 7.6.5, Elliptic Curve Cryptography (ECC) certificates are introduced for their superior security-to-size ratio, which allows for stronger encryption with smaller, more efficient keys. A 256-bit ECC key can offer the same security as a 3072-bit RSA key.

Remote API target and SAML target are not used for ECC certificate.

For RADIUS RadSec and Local RADIUS Server (EAP) feature, the ciphers TLS_AES_256_SHA384 and TLS_AES_128_SHA256 should be selected to support ECC certificates which are signed by ECDSA secp384r1 and secp256r1.

Note: Microsoft Entra does not support ECC. Currently, ECC certificates are not applicable for SAML and Remote API targets.

8. Enter the remaining information for the certificate in the dialog box:
 - **Organization:** The name of the server's organization.
 - **Organizational Unit:** The name of the server's unit (department).
 - **Locality (City):** The city where the server is located.
 - **State/Province:** The state/province where the server is located.
 - **2 Letter Country Code:** The country code where the server is located.
9. Click **OK** to generate the CSR.
10. Copy the section with the certificate request to include the following:


```
-----BEGIN CERTIFICATE REQUEST-----
...Certificate Request Data...
-----END CERTIFICATE REQUEST-----
```
11. Paste it into a text file, and save the file with a .txt extension. Note the location of this file on your PC. Make sure there are no spaces, characters, or carriage returns added to the certificate.
12. Send the certificate file to the CA to request a valid SSL certificate.

Important Notes:

- Do not click OK in the Generate CSR screen after saving the certificate file and sending to the CA. Each time OK is clicked on the Generate CSR screen, a new CSR and private key are created, overwriting any previous private key. Consequently, if a certificate file has been submitted to the CA, and **OK** has been clicked since the original certificate was generated, the returned certificate will not match the current private key, and a new request will have to be issued and sent to the CA.
- Not all certificate Authorities ask for the same information when requesting a certificate. For example, some CA's ask for a server type (Apache, etc) while others do not. FortiNAC requires a non-encrypted certificate in one of the following formats:
 - PEM
 - DER
 - PKCS#7
 - P7B
 - PKCS#12

This will allow the certificate to be applied to any of the desired components.

If the certificate is in PEM format, opening the certificate in a text editor should look something like the following format:

```
-----BEGIN CERTIFICATE1-----
fjkghwjernlsfuigylerkjlkfjnu23jnlkjblu5ghl6kh4
fjkjlkfjnu23jnlkjblu5ghl6khkghwjernlsfuigyler4
ghwjernlsfuigylerkjlkfjnu23jnlkjblu5fjkghl6kh4
-----END CERTIFICATE1-----
-----BEGIN CERTIFICATE2-----
fjkghwjernlsfuigylerkjlkfjnu23jnlkjblu5ghl6kh4
fjkjlkfjnu23jnlkjblu5ghl6khkghwjernlsfuigyler4
ghwjernlsfuigylerkjlkfjnu23jnlkjblu5fjkghl6kh4
-----END CERTIFICATE2-----
```

Certificate requests generated on FortiNAC use the SHA1 RSA encryption signature. However, certificates with SHA2 encryption can be requested using this CSR.

Upload the certificate

Upload the valid SSL certificate to the appliance when the certificate file is returned from the CA. Certificate files can be returned to you in one of several configurations. Depending upon the CA, one or multiple certificate files may be returned.

1. Save the file(s) received from the CA to your PC.
2. Select **System > Certificate Management**
3. (If this appliance is in a HA group) Select the server to which the certificate will be applied.
4. Click **Upload Certificate**.
5. Select the certificate target to which the certificate will be applied.
6. Select a certificate file type: **Certificate** or **PKCS #12 Certificate**.
 - a. When Certificate type is selected:
 - Select **Use Private Key from Last Generated CSR** to use the key from the most recent CSR for the selected target.
 - Select **Reuse Private Key from Existing Certificate** to use the private key for the certificate currently in use. This option is for renewing an existing installed certificate.
 - Select **Upload Private Key** to upload a key stored outside FortiNAC. Click **Choose** to find and upload the private key.
 - b. When PKCS #12 Certificate is selected:
 - In **Password** field, enter the password of the PKCS#12 certificate file.
7. Click **Browse** to find and select the certificate or the PKCS#12 certificate file to be uploaded. Users can also upload CA certificates and CA bundles.

Upload any relevant intermediate certificate files needed for the creation of a complete certificate chain of authority. The CA should be able to provide these files. Without a complete certificate chain of authority, the target functionality may produce error/warning messages.
8. Click **Add Certificate** if multiple certificates were returned. Use this to enter each additional certificate file.
9. Click **OK**.

Download a certificate

SSL server certificates are available to download in PEM or PKCS#12 format. Only PEM certificates can be downloaded through FortiNAC administrator while both PEM and PKCS#12 certificates can be downloaded through FortiNAC CLI.

Download PEM certificate through FortiNAC Administrator

1. In FortiNAC administrator, go to **System > Certificate Management > Server Certificates**, and click on **Server Certificates** button on the right.
2. Select a **Certificate Target** and click **Download**.
3. The certificate in PEM format will be download to the local server or machine with a default name `"certificate.cer"`.

Download certificates in PEM or PKCS#12 format through FortiNAC CLI

- Server certificates in PEM or PKCS#12 can be exported to a remote server through SCP, FTP, and TFTP commands.
- When exporting certificate in P12 file format, the file contains a certificate and a private, the password parameter is required.
- PEM file is *.cer file and does not require the "p12-password" parameter. The default password is "fortinet".
- The optional parameter "applied-to" is only applicable to HA: primary/secondary and self. The default is self.

File Transfer Protocol	Complete File Transfer CLI Command
SCP	execute export certificate scp <certificate-format> <certificate-alias> <filepath> <server>[:port] <username> <password> [--appliedTo <appliedTo>] [--p12Password <p12Password>]
FTP	execute export certificate ftp <certificate-format> <certificate-alias> <filepath> <server>[:port] <username> <password> [-appliedTo <appliedTo>] [--p12Password <p12Password>]
TFTP	execute export certificate tftp <certificate-format> <certificate-alias> <filepath> <server> [--appliedTo <appliedTo>] [--p12Password <p12Password>]

Example: Transfer a PKCS#12 certificate via SCP:

```
execute export certificate scp PKCS12 radsec /var/ftp/zjian 10.15.33.7 ftp user --appliedTo self --p12Password fort
```

Copying a certificate to another target

If the certificate is intended to be used for multiple targets, copy the certificate to the new target:

1. Highlight the target with the desired certificate installed.
2. Click **Copy Certificate**.
3. (If this appliance is in a HA group) Select the server to which the certificate will be applied.
4. Select the new target from the drop-down menu.
5. Click **OK**.

Activating portal certificates (vF7.2.5 and lower)

Certificates for the and Portal (vF7.2.6 and above), Admin UI and Persistent Agent are activated automatically upon installation. No further action is required.

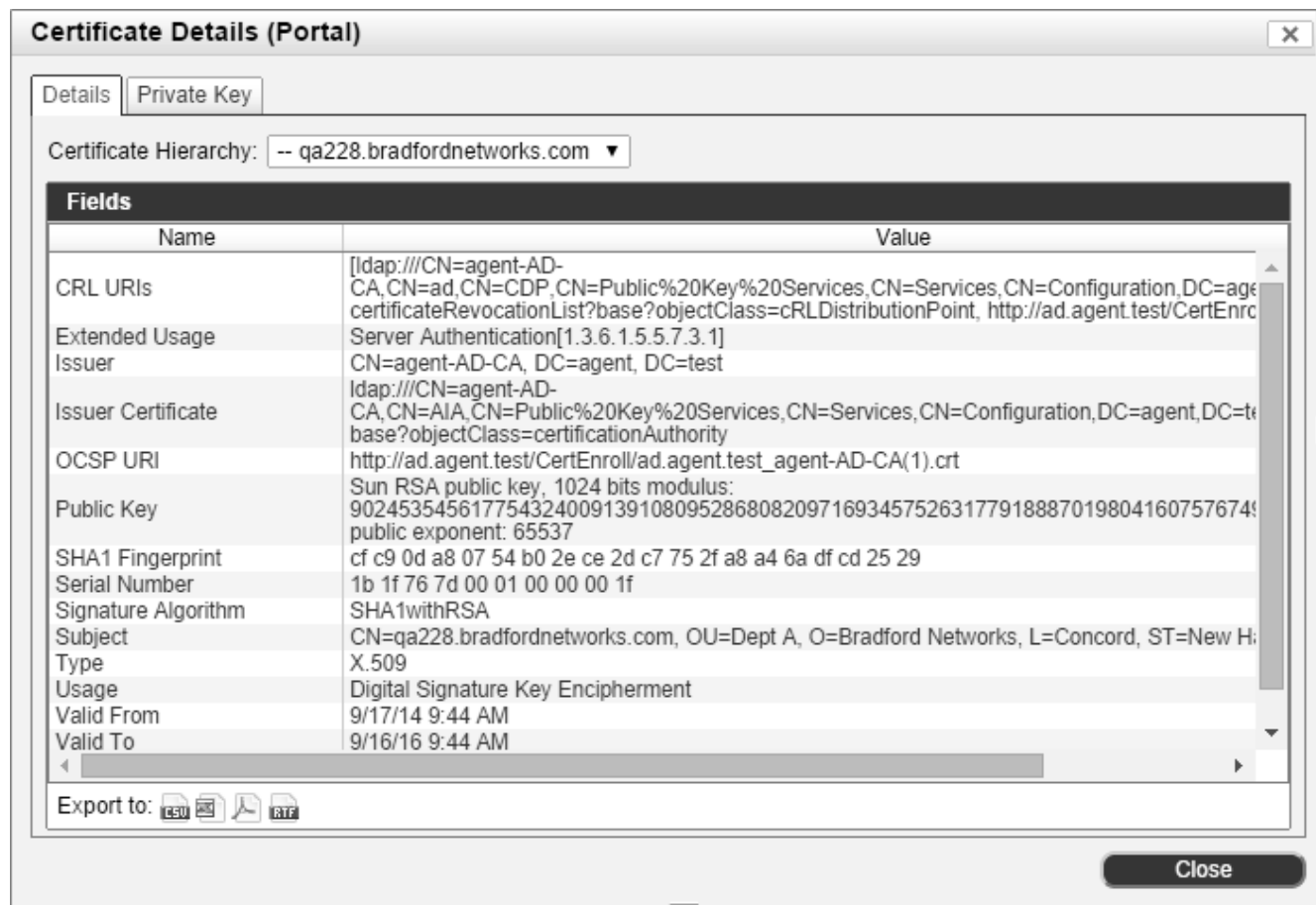
To begin using the certificate when connecting to the Portal, do the following:

1. Navigate to **Portal > Portal SSL**
2. In the **SSL Mode** field, select **Valid SSL Certificate**.
3. Click **Save Settings** (this may take several minutes).

View details of a certificate

View the details and private key information for a certificate

Users can view the certificate details and private key information for the selected target.



1. Click **System > Certificate Management**
2. Click **Details**.

Trusted certificates

Use this view to upload certificate authority (CA) certificates in order to establish trust for SSL connections.

NOTE: Installing certificates under the Server Certificates tab does not automatically add the root/intermediate certificate to the corresponding target under the Trusted Certificates tab.

Example:

Server Certificates tab Certificate Target: "Local RADIUS Server (RadSec)"

Corresponding Trusted Certificates tab Target "RADIUS Endpoint Trust (RadSec)"

1. Navigate to **System > Certificate Management**.
2. Select **Trusted certificates**.
3. (If this appliance is in a HA group) Select the server to which the certificate will be applied.
4. Select the appropriate target from the drop down menu using the table below.

Target	Description
F 7.6.2 and below	For future use.
RADIUS Endpoint Trust [RadSec]	Trusted Endpoint Certificate used by FortiNAC to validate the client-side certificate when RadSec clients send authentication requests.
RADIUS Endpoint Trust [radius]	Trusted Endpoint Certificate used by FortiNAC to validate the client-side certificate when Local RADIUS Server is configured and EAP-TLS is used for authentication. See below for additional details.
SAML Trust (Admin) (F 7.6.3 +)	Trusted Endpoint Certificate used by FortiNAC to validate administrators that log in to the FortiNAC administrative UI using IdP credentials. See SAML SSO integration guide for details: https://docs.fortinet.com/document/fortinac-f/7.6.3/saml-ssol
SAML Trust (User) (F 7.6.3 +)	Trusted Endpoint Certificate used by FortiNAC to validate end users authenticating through the Captive Portal using IdP credentials. See SAML SSO integration guide for details: https://docs.fortinet.com/document/fortinac-f/7.6.3/saml-ssol
General Trusted CA	Used by FortiNAC to validate SSL connections with devices modeled in Inventory. Used when SSL Settings in the Credentials tab is configured. See Credentials. Well-known trusted CA certificates can be imported to this view automatically. For details, see Certificate Management .
WinRM Trusted CA Chain	Trusted endpoint certificate used by FortiNAC to validate the client-side certificate for WinRM sessions. Applies to Device Profiling Rules using WinRM or WMI Profile methods. See Adding a rule .
Persistent Agent Cert Check	Trusted CA certificate used by FortiNAC to validate certificates on Windows hosts. See Certificate validation .

5. Click **+** then browse to add the certificate file for the selected target. Click **+** for each additional certificate required.
6. Click **OK**.

RADIUS Endpoint Trust [radius]

EAP-TLS is a certificate-based mutual authentication method. When using EAP with TLS certificates, both the client and the server use certificates to verify identities to each other. Once these certificates are identified, the EAP-TLS will create session-based keys that each party can use to complete the login.

Endpoint Trust Certificate used by FortiNAC to validate the client-side certificate when local RADIUS server is configured, and EAP-TLS is used for authentication.

The SSL certificates requirements for Endpoint Trust:

- The incoming certificate must be issued by Root CA.
- 3rd party public or corporate owned internal Certificate Authority issued certificates.
- Wildcard certificates are not recommended.
- Either user or computer certificates.
- Supported using EAP-TLS, PEAPv0-EAP-TLS, EAP-TTLS/EAP-TLS, and TEAP
- Multiple certificates can be uploaded to FortiNAC for this use.

Client will be unable to authenticate unless the RADIUS Endpoint Trust Certificate Target has the matching root certificate installed. All the root certificates used by end stations should be uploaded to FortiNAC.

- Acquire the root certificate(s) used by the endstations.
- If multiple root certificates have been distributed, ensure each one has been collected.

FortiNAC		tb40.nacqa.test		admin	
Dashboard	>	Upload Certificate	Details	Delete	
Users & Hosts	>	Certificate Target		Issued By	
Network	>	RADIUS Endpoint Trust [radius]		client	
Policy & Objects	>	RADIUS Endpoint Trust [radius]		radius	
Portal	>	RADIUS Endpoint Trust [Self_signed]		Self_signed	
Logs	>	RADIUS Endpoint Trust [Self_signed]		nacqa.test	
System	>				
Certificate Management	>				
Config Wizard	>				

The root certificate of user certificate for RADIUS endpoint should be uploaded to Trusted Certificate of FortiNAC. FortiNAC will verify the client certificate based on the root certificate stored on FortiNAC.

On the RADIUS 802.1x Endpoint, user needs to apply the user certificate and private key to let the FortiNAC verify the user. The private key must have password protected.

And the user also needs to apply the root certificate of RADIUS Server certificate to let the end point verify the certificate of FortiNAC.



The self-signed certificate whose common name is same as issuer cannot be used in here. Otherwise, there is a error message: "ERROR: SSL says error 18 : self signed certificate" on RADIUS server log."

The screenshot shows the 'Wired' network configuration window with the 'Security' tab selected. The '802.1x Security' toggle is enabled. The 'Authentication' dropdown is set to 'TLS'. The 'Identity' field contains the text 'atest1'. The 'User certificate' field displays 'client-cert.pem'. The 'CA certificate' field displays 'ca.pem' and includes an unchecked checkbox for 'No CA certificate is required'. The 'Private key' field displays 'client-key.pem'. The 'Private key password' field is masked with dots, and there is an unchecked checkbox for 'Show password'.

The self-signed certificate cannot be used for RADIUS Endpoint. The RADIUS Server will verify the common name of the root certificate and user certificate. If the two common names are same, there is an error "ERROR" SSL says error 18: Self signed certificate" on RADIUS Server.

If the user certificate is not issued by root CA or the root Certificate is not uploaded to FortiNAC, there is an error "ERROR: TLS Alert read: fatal: unknown CA" on RADIUS Server.

Notes on High Availability

Starting from FortiNAC 7.6.3, FortiNAC supports configuring (generating, uploading, or copying) certificates used on the secondary server of a 1+1 or N+1 HA group directly from the primary server's GUI. Users can also configure the certificates used on the primary server from the secondary server's GUI, provided the secondary server is in control. All configured certificates will be synchronized between the primary and secondary servers.

For more information on High Availability, see the [1+1 HA documentation](#) and the [N+1 HA documentation](#).

In the certificate lists, the "Applied to" field shows which server the certificate applies to (Primary or Secondary).

Further explanation of the "Applied to" field:

- If the server is a primary server:
 - **Primary:** The certificate is applied to this primary server.
 - **Secondary:** If this primary server fails, this certificate is applied to the secondary server when it takes control.
- Note:** In an N+1 HA group with multiple primary servers, each primary server may synchronize a different certificate to the secondary.
- If the server is an in-control secondary server:
 - Primary:** The certificate is applied to the primary server that this secondary server has taken control from.

Secondary: The certificate is applied to this secondary server.

Note: In an N+1 HA group, if the secondary has taken control from a different primary server, the applied certificate may differ.

The certificate management page is not available in the secondary server's GUI unless it is currently in control.

A certificate can only be used on one server. If you want to use the same certificate on both the primary and secondary servers, you must copy it from one server to the other.

Config wizard



IPv6 is for demo purposes only.

Use Config Wizard for setting up the following in the FortiNAC server:

- Initial license key installation (VMs only)
- Basic Network Configuration
 - Host Name
 - Port1 IP address, mask and default gateway
 - DNS
 - NTP and TimeZone
- Network Type (Layer 3, Layer 2 or None)
- Isolation interface (port2)
 - Port2 IP address, mask and default gateway
 - DHCP scopes & attributes
 - Pre-boot Execution Environment (PXE)
 - Isolation IP Subnets
 - Additional Routes

If configurations need to be reviewed or modified once completed, Config Wizard can be accessed in the GUI under **System > Config Wizard**.

For details on implementing Config Wizard, refer to the [Config Wizard reference manual](#) in the Document Library.

Note: The data displayed in the Config Wizard may not represent the current configuration of the appliance. When making edits in the Config Wizard, modifications are stored in a temporary file. This allows users to exit the Config Wizard before saving changes permanently.

Cluster Management

Navigation: **System > Cluster Management**

FortiNAC Manager provides users a central access service to view or modify multiple CA's information, including endpoints, configuration, etc. The cluster solution is needed because more and more CA's are required for certain use cases and a single FortiNAC Manager can no longer process all the information timely and effectively.

Each FortiNAC Manager node in the cluster can be either one of the following types:

- Leader
- Worker

Leader Node	Worker Node
Each cluster only has one leader node	Each cluster can have multiple worker nodes
Responsible for sending heartbeat to worker nodes and exchanging information	Responsible for providing information to leader node, such as database information, via heartbeat
Leader node can be transferred to worker nodes if there are no worker nodes associated with it	Worker node can be transferred to a leader node if there is no leader node in the cluster
Worker nodes can only be added into the cluster through a UI hosted by leader node	

FortiNAC Manager can be set to worker node or leader node, which is not in any cluster.

In the leader node, the properties about the nodes are follows:

Name	The name given to the node when the user configures FortiNAC Manager
Status	Running, Reconnecting, Disconnected, Initializing
Node Type	Leader, Worker
NAC-M Capacity	The capacity of CAs that FortiNAC Manager can accommodate and has managed
CA Managed By	The number of CA that managed by this FortiNAC Manager node
Port1 IP Address	The MGMT port IP address of FortiNAC Manager
Serial #	The FortiNAC Manager serial number
Version	The version of FortiNAC Manager
Shared IP	In a cluster of multiple NCM's, when the leader switches during failover, the shared IP can automatically access the new leader.
Remove Shared IP	Get rid of the Shared IP.

Modify Nodes

Add New

In leader node, the user can add worker node to this cluster.

1. Click **"Add New"**.
2. Enter the name of worker node.
3. Enter the port1 IP address of worker node.
4. Enter the serial number of worker node.
5. Click **"OK"** to finish this operation.

Edit

In leader node, users can select a node to edit.

If the user selects the leader node to edit, the user will be redirected to the "Config Wizard" page. For detailed operations, see the "Config Wizard" section.

If the user selects the worker node to edit, the user could edit the "Name" and "Port1 IP Address".

Delete

A leader node cannot be deleted.

In leader node, the user can only delete a node when the following apply:

- Node is a Worker.
 - Worker node is not managing any CAs. ("CA Managed By" value is 0).
 - A worker node does not have the endpoint license installed. See [License Management](#).
1. Select a worker node.
 2. Click **Delete**.
 3. Click **OK** to confirm the operation on pop up dialog.

Search & Group By

FortiNAC Manager search dialog box accepts keywords entered by the user and dynamically display options containing these keywords.

FortiNAC Manager can group all nodes according to the following attributes:

- Status
- Node Type
- NAC-M Capacity
- CA Managed By
- Port1 IP Address
- Serial #
- Version
- Name

Switch Worker to Leader

There are two ways to set a worker node as leader node, and then the original leader node become worker node.

Manual Operation

1. Select a worker node.
2. Right click the worker node.
3. Click **Make Leader**.
4. Click **OK** to confirm.

Automatic Operation

When the leader node is down or offline, other worker nodes will randomly select a CA register to the leader node and validate its status. If the status is Reconnecting/UN-Reachable, then the leader node will be marked as Reconnecting by work nodes. If the status remains 15 minutes, the status will be then marked as Disconnected. Thus, the worker node who joins the cluster first will be elected as the new leader.

When the original leader node is back, it becomes a worker node.

Rebalancing

When a node status changed to Disconnected, the leader node will rebalance and redistribute its CA to other nodes.

If a node's status changed from Disconnected to Running, the CA's that were originally registered to the recovered node will be assigned back to it.

Endpoint Synchronization

FortiNAC Manager will actively pull endpoint information (users, hosts, and adapters) from each managed CA every 5 minutes, incrementally, and save them locally. The information will only be synchronized to CA when needed. When an endpoint device registers from CA1 to CA2, its information will be retrieved from FortiNAC Manager to CA2.

Groups

Groups allow you to put like items together. By creating groups you eliminate the need to configure and control items within the group individually. For example, if you put a set of ports in a group, you can modify the group settings and affect all of the ports simultaneously. Groups can contain other groups.

Use the Groups view to add, modify, and delete groups within FortiNAC. FortiNAC comes with some standard groups over which it maintains ownership. These are marked as system groups. Create user-owned groups to group devices, ports, hosts or users. Associate these groups with scheduled tasks to perform a variety of functions.

Groups can be used to assign policies or roles to hosts or users.

If there are more than 2000 groups in the database, the groups are not automatically displayed. Instead, a confirmation dialog is shown asking if you would like to continue. Note that large numbers of records may load very slowly if not filtered. Choose **Yes** to display all groups or **No** to reduce the number displayed by using the filters.

Settings

Field	Definition
Name	Name used to identify the group.
Type	Indicates whether this is a group of ports, devices, IP phones, hosts, users or administrators.
Owner	Creator of the group. System indicates that the group was created by FortiNAC. User indicates that an administrator created the group.
Members	The number of items contained within the group. For example, if this is a host group, this number indicates the total number of hosts in the group. If this group contains sub-groups, the number includes those items in each sub-group.
Days Valid	This column only applies to Host groups. The Expiration Date for hosts in this group is calculated using the number of days valid. For example, if a host is added to the group on 01/01/2011 and days valid is set to 30, the host's Expiration Date is set to 01/31/2011. The Expiration Date is set when a host is added to the group or when the Days Valid is edited. See Aging hosts in a group on page 851 for more information.
Days Inactive	This column only applies to Host groups. The number of days of network inactivity after which hosts in this group are removed from the database. For example, if this is set to three and a host in this group has not connected to the network for three days, the host record is removed from the database. See Aging hosts in a group on page 851 for more information.
Description	User specified description for the selected group.
Last Modified By	User name of the last user to modify the group.
Last Modified Date	Date and time of the last modification to this group.
Synced from LDAP	Indicates if group was manually created or imported from LDAP. Imported groups have the check box selected under the Select Groups tab of the LDAP configuration (System > Settings > Authentication > LDAP).

Field	Definition
	Upgrading from pre-F7.6 version: The default value for this field is 'false'. A green check mark displays after the next directory synchronization post upgrade.
Right click options	
Copy Group	Creates a copy of the selected group.
Delete	Deletes the selected group.
Group Member Of	Displays groups in which this group is a member. A group can be a sub-group of another group of the same type. See Group membership on page 847 .
In Use	Provides a list of other features that reference this group, such as a Policy Mapping or a Scheduled Task. See Group in use on page 851 .
	 System-owned groups will not be displayed as "In Use", even though they are in use by the system.
Manages	Applies only to administrator groups. Administrator groups can be designated to manage groups of devices or hosts. See Limit user access with groups on page 846 .
Modify	Opens the Modify Group window. See Modify a group on page 846 .
Set Host Registration Limit	This feature is only available to User and Administrator Type groups. Administrators can define limits to the number of registered hosts allowed per user within the group.
Modify Device Properties	Applies only to device groups. Allows you to modify multiple devices at the same time.
Set Aging	Allows you to set Days Valid and Days Inactive for the selected host group. Days valid and days inactive are used to calculate the date when the host is aged out of the database. Date is set when a host is added to the group or when the fields are modified. See Aging hosts in a group on page 851 .
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746 .
	 You must have permission to view the admin auditing log. See Add an administrator profile on page 139.
Buttons	
Show Members	Opens the Group Members window and displays a list of all of the items within the group. Indicates whether the item is a member of the main group or a sub-group. See Show group members on page 851 .

Add groups

Create additional groups to logically group elements that require network resources.

1. Select **System > Groups**.
2. From the Group view, click **Add**.
3. Enter a **Group Name**
4. Select a **Member Type**, which indicates the types of items that will be included in the group.

Type	Description
Administrator	Administrators that access FortiNAC.
Hosts	Hosts that access the network.
Devices	Devices such as switches, computers, or printers.
Ports	Ports on switches on the network.
Users	Users that log onto the network.

5. For Host groups you have options for **Days Valid** and **Days Inactive**. These fields are used to calculate the expiration date used to age hosts out of the database. They are optional and should not be set if you have another mechanism that sets the expiration date. See [Aging out host or user records on page 241](#) before you set these fields.
6. Enter a **Group Description**.
7. In the **All Members** pane select one or more items to be included in the group, then click the right arrow to move them to the **Selected Members** pane. For lists that do not include check boxes, select multiple items by holding down the **Ctrl** key while clicking.
8. To remove an object from the group, click on it and then click the left arrow.
9. To add subgroups to a group, select the **Groups** tab and select one or more groups to add as subgroups.
10. Click **OK** to save the new group.

Copy a group

1. Select **System > Groups**.
2. Locate the group to be copied.
3. Right-click on the group and select **Copy Group**.
4. Enter a name for the new group and click **OK**.
5. The new group appears in the **Groups View**. This group is owned by the user and not FortiNAC.

Delete a group

1. Select **System > Groups**.
2. Locate the appropriate group.
3. Right-click the group to select it and choose **Delete** to remove the group from the list.
4. Click **Yes** to confirm that you wish to delete the group.

Limit user access with groups

To control which hosts and ports administrators can access you can place those administrators in special groups. Then designate those special Admin groups to manage groups of hosts or ports.

Example:

Assume you have two administrators that are responsible for monitoring medical devices and nurses in a hospital. They should not see any other data. To accomplish this you must configure the following:

- Place the nurses' workstations into a host group.
- Place the medical devices to be monitored into a host group.
- Place the ports where the medical devices connect into a port group.
- Place these two administrators in a special administrator group.
- Assign these two administrators to a profile with permissions for Manage Hosts & Ports. Make sure the **Manage Hosts & Ports** setting on the General Tab of the profile is set to **Restrict by Groups**.
- Set the Administrator group to manage the nurses group, the medical device group and the port group.
- Remove these two administrators from the All Management Group or they will have access to all hosts and ports.

When those administrators log into the admin UI, they can only see data associated with the nurses, medical devices or the ports in the groups they manage.



Make sure to remove affected administrators from the All Management group or they will continue to have access to all hosts and ports.



Administrators can still view all hosts and users from the Locate View if their administrator profile gives them permission for that view, but they can only modify those that are in the group they are managing.

-
1. Create the group of hosts or ports. See [Add groups on page 845](#) for instructions.
 2. Create an administrator profile with permissions for Manage Hosts & Ports. Make sure the **Manage Hosts & Ports** setting on the **General Tab** of the profile is set to **Restrict by Groups**. See [Add an administrator profile on page 139](#).
 3. Create an Administrator group that contains the administrators responsible for the devices or ports.
 4. Remove the administrators from the All Management group. See [Modify a group on page 846](#) for instructions.
 5. Right-click on the Administrator group of administrators and select **Manages**.
 6. On the **Manages** window, select the group(s) to be managed by marking them with a check mark.
 7. Click **OK**.

Modify a group

Modify a group by adding additional items to the group or removing members from the group. Group description, days valid, and days inactive can also be modified.

1. Select **System > Groups**.
2. Select the group.

3. Click **Modify**.
4. If this is a host group, **Days Valid** and **Days Inactive** can be modified. See [Aging out host or user records on page 241](#) before modifying these numbers.
5. To add members to the group, Ctrl-click items in the **All Members** panel, then click the right arrow.
6. To remove items from the group, Ctrl-click items in the **Selected Members** panel, then click the left arrow. All items can be removed from the group by clicking the double left arrow.
7. To modify subgroups, click the **Groups** tab and check or uncheck groups in the displayed list.
8. When you have made all desired modifications for the group, click **OK**.

Group membership

Displays the groups that contain the selected group and allows you to modify group membership. For example, if you had a group called Staff, you might want to further sub-divide that by department, therefore you could have sub-groups such as Accounting or Human Resources within Staff. Selecting **Human Resources** from **Groups** and opening the **Group Membership** window would show that hierarchy. In addition the selected group can be added to or removed from other groups.

1. Select **System > Groups**.
2. Locate the appropriate group.
3. Right-click the group to select it and choose **Group Member Of** to display the groups that contain the selected group.
4. Modify the groups as needed and click **OK** to save your changes.

Set Host Registration Limit

Set Host Registration Limit allows configuration on the number of registered hosts allowed per user in a group. The type of group is only limited to **User** or **Administrator**. This feature provides granular control over the number of devices allowed to be registered by a user and the type of devices (Desktop PC, Mac, Laptop, Phone, etc.).

For example, a user can be allowed to register 1 Macbook, 1 PC desktop, and an iphone.

Steps to Setup Host Registration Limit

1. Right click on a group with **User** and **Administrator** type and select **Set Host Registration Limit**.
2. Click **+Add New** to select either **Limit by Role** or **Limit by Device Type**.

Set Registered Host Limit ✕

Exclude MDM Devices ? 🔴

Registered Host Limit

+ Add New ▾

Edit

Delete

+ 🔍 Search

Q

Rank	Set Limit By	Role/Device Type	Max Number of Registered Hosts
1	Role	NAC-Default	1
2	Role	BYOD	1
3	Device Type	macOS	1
4	Device Type	Windows	1
5	Device Type	Linux	1

3. Option 1: When **Limit by Role** is selected, a separate window is open where the role and the maximum number of registered hosts can be selected.

Add New Limit by Role

Rank

6

Role

Search

Q

+

Roles ▾

BYOD
Contractor
Guest
GuestAccess
GuestConference
GuestSelfRegistration
NAC-Default

Max Number of Registered Hosts

4. Option 2: When **Limit by Device Type** is selected, a separate window is open where the device type and the maximum number of registered hosts can be selected.

Add New Limit by Device Type

Rank: 6

Device Type: [Dropdown Menu]

Max Number of Registered Hosts: [Input Field]

Search [Input Field]

DeviceTypes [Dropdown Menu]

- Alarm
- Alarm System
- Android
- AP
- Apple iOS
- Appliance
- Arduino
- Audio Player
- Automotive
- Baby Monitor
- Barcode Scanner
- Blood Analyzer

5. Both **Limit by Role** and **Limit by Device Type** are evaluated by their ranking, and depending on which limit triggers first will generate an alert and block host registration.

Host Registration Limit Reached

When a user attempts to register a new host device but a limit is already reached, the captive portal window will display the following error, and a notification e-mail will be sent to the user.



Configuration Exception

Edit Limit by Role Exception - When configuring host registration limit by role exception, it can happen when the new limit is lower than the number of hosts registered by the user on FortiNAC. An error message with a CSV file showing number of hosts registered under the user is available for download. The new setting will not be saved.

The screenshot shows the FortiNAC configuration interface. On the left, the 'Set Registered Host Limit' panel is visible, showing a table with columns 'Rank' and 'Set Limit'. The table has 5 rows, with the first row selected. The 'Set Limit' column shows 'Role' for rank 1, 'Role' for rank 2, 'Device Type' for rank 3, 'Device Type' for rank 4, and 'Device Type' for rank 5. On the right, the 'Edit Limit by Role' panel is open. It shows 'Rank' set to 1, 'Role' set to 'NAC-Default', and 'Max Number of Registered Hosts' set to 1. A yellow error message box is displayed, stating: '# Users/Admins of NAC-Default Role have more than # Registered Hosts within this group. Click the download button to download full list.' Below the message is a 'Download' button. At the bottom of the panel are 'OK' and 'Cancel' buttons.

Rank	Set Limit
1	Role
2	Role
3	Device Type
4	Device Type
5	Device Type

Edit Limit by Device Exception - Similarly, when the modified device host registration limit is lower than the current registered host, an error message will be displayed, and the new setting will not be saved.

The screenshot shows the FortiNAC configuration interface. On the left, the 'Set Registered Host Limit' panel is visible, showing a table with columns 'Rank' and 'Set Limit'. The table has 5 rows, with the third row selected. The 'Set Limit' column shows 'Role' for rank 1, 'Role' for rank 2, 'Device Type' for rank 3, 'Device Type' for rank 4, and 'Device Type' for rank 5. On the right, the 'Edit Limit by Device Type' panel is open. It shows 'Rank' set to 3, 'Device Type' set to 'macOS', and 'Max Number of Registered Hosts' set to 1. A yellow error message box is displayed, stating: '# Users/Admins have more than # Registered Hosts of macosx within this group. Click the download button to download full list.' Below the message is a 'Download' button. At the bottom of the panel are 'OK' and 'Cancel' buttons.

Rank	Set Limit
1	Role
2	Role
3	Device Type
4	Device Type
5	Device Type

Show group members

This option displays a list of all of the items within the selected group. Indicates whether the item is a member of the main group or a sub-group.

1. Select **System > Groups**.
2. Select the group and click **Show Members** to display the list of items within the group.
3. Use the **Find** field to search for a particular item by typing in any part of its name and clicking **Next** or **Previous**. This field is case sensitive.

Group in use

To find the list of FortiNAC features that reference a group, select the group from the Groups View and click **In Use**. A message is displayed indicating whether or not the group is associated with any other features. If the group is referenced elsewhere, a list of each feature that references the group is displayed.



System-owned groups will not be displayed as "In Use", even though they are in use by the system.

Aging hosts in a group

Use the Set Aging window to set aging for the hosts in a selected Host group. Using the Aging feature populates the Expiration Date and the Inactivity Date fields on the **Host Properties** window. Hosts with existing age times are modified. This option is only valid for Host groups. If a host is a member of more than one group, the aging time is applied based on the last group to which the host was added or the last group whose aging times were modified.

Adding age times to existing hosts can cause some hosts to be removed from the database immediately depending on the creation date of the host record. If, for example, the creation date is 01/01/2010, today's date is 02/02/2010 and Days Valid is set to 5, then the Expiration Date calculated is 01/06/2010. The record is deleted immediately.

If hosts have been manually set to Never Expire, the Expiration Date and Inactivity Date fields for those hosts will not be modified by adding those hosts to a group with aging settings. See [Properties on page 221](#), [Set host expiration date on page 233](#) and [Aging out host or user records on page 241](#) for additional information.

1. Select **System > Groups**.
2. Right-click on the host group and select **Set Aging**.
3. Enter a number for **Days Valid** or **Days Inactive**. The number in days valid is used to calculate the expiration date for each host in the group. The number in days inactive is used to calculate the inactivity date for each host.
4. Click **OK**.

System groups

The groups listed below are default system groups that exist within the FortiNAC database. They cannot be deleted. Some groups need to be fine tuned to your network. Details are included in the table below.

Group	Definition
Administrator	
All Management	FortiNAC administrators with all management access rights. Initially contains only admin and root. New administrators are added to this group automatically. This is the default group for e-mail notifications triggered by alarms. Add users to your own specific Administrator groups to give them privileges to manage (disable and enable) specific hosts and ports. If you place a user into your own Administrator group, be sure to remove that user from the All Management group. See Limit user access with groups on page 846.
Port	
Access Point Management	Ports with authorized access points connected and FortiNAC serving DHCP. Examples are dumb hubs or wireless units. FortiNAC provides management of hosts connecting through these access points.
Authorized Access Points	Ports that have authorized access points connected. Access points that connect to these ports do not generate Multi Access Point Detected events or alarms and the port is not switched to another VLAN during, for example, Forced Registration or role management VLAN Switching. Access points that connect to ports that are not in this group do generate an event or alarm. Add switch ports that connect to hubs and wireless access points to this group.
Forced Authentication	Ports that participate in forced authentication when unauthenticated users connect. If you have a port in this group, when a host connects to this port and is unauthenticated, the port is put into isolation VLAN and the host is forced to authenticate.
Forced Registration	Ports that participate in forced registration when unregistered hosts connect. Add switch ports that participate in forced registration when an Unregistered Host connects to the Forced Registration port group. Only ports that participate have their VLAN ID set to the Registration VLAN when an Unregistered Host connects.
Forced Remediation	Ports that participate in forced remediation VLAN switching when hosts connect.
Reset Forced Default	Ports that return to the default VLAN when hosts disconnect.
Reset Forced Registration	Ports that return to Registration when hosts disconnect.
Role-Based Access	Ports that participate in role-based access and switch VLANs, based on the role of network devices, such as printers, when they connect. Add switch ports that participate in VLAN switching. Ports that participate have their VLAN ID set to the role specified for the connected network device. Example: A printer is set up with the role "Accounting". When the printer connects to a port in this group, the printer is switched to the VLAN associated with the "Accounting" role.

Group	Definition
System DHCP Port	The port used to discover unauthorized DHCP servers and validate authorized DHCP servers.
Temporary Port Exception Group	A system-defined group in FortiNAC that allows users to exempt specific ports from policy enforcement for a set period. During this time, devices on these ports operate as rogue devices, connecting to the default VLAN, and automatically revert to their original enforcement group once the exception period ends.
Device	
Authorized DHCP Servers	Servers that are authorized to serve DHCP on the network.
Bridging Devices	Devices that support the SNMP bridging MIB.
	 This group has been replaced by the L2 network devices group.
Device Interface Status	Devices created through Discovery or created manually are automatically added to this group. Use this group in conjunction with the task scheduler to periodically update the interface status for each device in the group.
L2 Network Devices	Devices that support the Standard 802.1d Bridge Table. This group is also used for filtering the list of devices displayed on the L2 Network Devices window. As new L2 devices are discovered they are added automatically to this group and to either L2 Wired Devices or L2 Wireless Devices.
L2 Wired Devices	A sub-group of L2 Network Devices that is used for filtering on the L2 Network Devices window. L2 Wired Devices are added to this group automatically as they are discovered. Note: Removing a device from this group does not disable L2 (Hosts) Polling under the Polling tab in Inventory.
L2 Wireless Devices	A sub-group of L2 Network Devices that is used for filtering on the L2 Network Devices window. L2 Wireless Devices are added to this group automatically as they are discovered. Note: Removing a device from this group does not disable L2 (Hosts) Polling under the Polling tab in Inventory.
L3 (IP-->MAC)	This group must be populated manually with your L3 devices. The L3 group can be used for filtering on the L3 Polling window.
Physical Address Filtering	Devices that participate in the enabling and disabling of hosts. Add switches that participate in host disabling to this group. If a host is connected to a switch that is not in the physical address filtering group, and that host is disabled through FortiNAC, the host remains connected to the network and is displayed as in violation. Add the switch regardless of whether a host is disabled through a Dead End VLAN, or through MAC address security.
Host view	

Group	Definition
Forced Scan Exceptions	Hosts that do not participate in forced scans.
Forced User Authentication Exceptions	Hosts that do not participate in forced user authentication.
Forced Remediation Exceptions	Hosts are scanned and can be marked "at risk", but are never put into remediation. Scan results are stored allowing the administrator to review the results and take corrective action without disrupting users on the network.
Global Agent Update Exceptions	Hosts in this group are excluded from automatic Persistent Agent Updates. Updates are controlled by MAC address. If a host has more than one MAC address, as long as any one of its MAC addresses is listed in this group the host is not updated.
Registered Hosts	Group of all registered hosts.
Rogue Hosts	This group has a special property that controls whether or not rogue hosts can access the network. Under Group Properties for this group, the Access field can be set to either Deny or Allow. • Deny: If the Access field is set to Deny, rogue hosts in this group are denied network access until they register and any new unregistered hosts are automatically put into the group as they connect to the network. • Allow: If the Access field is set to Allow, rogue hosts in this group are permitted to access the network and any new unregistered hosts are not added to the group. Devices that are not in the Inventory but are connected to managed switches are created as rogue hosts. If rogue hosts are denied access to the network, they are disabled. To prevent this from causing problems with new devices such as printers, lab hosts or servers, you must register them as devices or as hosts. See Register a host as a device on page 232 or Add or modify a host on page 227 for detailed instructions.

Customer defined groups

User-owned groups are typically created to associate devices, ports, IP phones or hosts. You can associate these groups with scheduled actions to perform a variety functions. Typical groups include the following:

Groups	Notes
Ports	Port groups can be used for a variety of purposes. Use the Fixed Day Task option in the Scheduler with the Disable Ports and Enable Ports actions to disable or enable ports on a date or time schedule. You can nest port groups to make it easier to add ports to the FortiNAC owned groups, such as Forced Registration groups.
Departments, Staff, Divisions	You can use Host groups for a variety of purposes. Use Disable Hosts and Enable Hosts on a date or time schedule with the Fixed Day Task option in the FortiNAC Scheduler. Nest host groups to make it easier to control access over large groups of students. Create host groups for each grade level to control each group through its own scheduled task. You can also create a host group that contains each grade level and schedule it to disable or enable the entire student population with a single task.

Groups	Notes
Administrator	This group contains administrators who can manage (disable and enable) ports or hosts contained in the associated port or host groups. For example, place administrator "John Smith" in the Northeast Admins group. Set the Northeast Admins group to manage the "Department 1 Ports" and the "Department 1 hosts". When John Smith logs in to FortiNAC, he can find and disable any host or port in those groups. See Limit user access with groups on page 846.

Feature Visibility

System > Feature Visibility provides the ability to enable or disable structural visibility changes to the FortiNAC style.

Option	Description
Unified Settings	Compress all four Settings views into a single Settings view under the System category
Legacy View Architecture	Switches views which have been upgraded back to the older FortiNAC style. Note: Legacy View Architecture is no longer supported in v7.6

Scheduler

Use the scheduler to add, modify and delete scheduled tasks within FortiNAC. A task is an action that is scheduled to occur at a specified time and is usually associated with a specific group.

There are two types of scheduling: fixed day and repetitive. A fixed day task is one in which you schedule a task to run on a combination of days of the week and times of the day, such as Mondays at 1:00 pm and Fridays at 10:00 am. A repetitive task is one that you schedule to start on a given day, at a certain time, for the number of times you specify, such as every 10 days starting today. You can set the repetition rate to any number of minutes, hours, or days.

Settings

Fields used in filters are also defined in this table.

Field	Definition
Enable Disable Buttons	Enables or disables the selected task.
Name	User created name for the task.
Action	Action being performed by the scheduler.
Group	Action is limited to the group listed.
Enabled	Indicates whether the task is enabled or disabled. Disabled tasks do not execute.
Schedule	Days and times that this task is scheduled to run.
Last Scheduled Time	Last time the task was executed by the scheduler.
Next Scheduled Time	Next time the task will execute.
Description	User specified description of the scheduled task.
Last Modified By	User name of the last user to modify the scheduled task.
Last Modified Date	Date and time of the last modification to this scheduled task.
Right click options	
Copy	Copy the selected task to create a new record.
Delete	Deletes the selected task.
Disable	Disables the selected task.
Enable	Enables the selected task.
Modify	Opens the Modify Scheduled Activity window for the selected rule.
Show Audit Log	Opens the Admin Auditing Log showing all changes made to the selected item. For information about the Admin Auditing Log, see Audit Logs on page 746 .

Field	Definition
	 You must have permission to view the Admin Auditing Log. See Add an administrator profile on page 139 .
Run Now	Executes the selected task immediately.

Add a task

1. Select **System > Scheduler**.
2. From the **Scheduler** view, click **Add**.
3. The **Enabled** check box is selected by default. Uncheck it if you want this task to be disabled.
4. Enter a **Name** for the task and an optional description.
5. In the **Action Type** field, select either **System** or **CLI**. System actions are predefined tasks that you can choose to execute. CLI actions are sets of command line instructions that are created in the CLI Configuration View and saved to be executed elsewhere in the program.
6. Select the **Action** from the list of system or CLI actions. Refer to the table below the instructions for more information.



See [CLI configuration on page 433](#) for information on creating CLI actions.

7. From the **Group** dropdown list, select the group that the action will be performed on. The list contains only the group types specific to that Action.
8. From the **Schedule Type** drop down list, select either **Fixed Day** or **Repetitive** and set the day and time that the task is to be performed.
9. A **Fixed Day Task** is one in which you schedule a task to run on a combination of days of the week and times of the day, such as Mondays at 1:00 pm and Fridays at 10:00 am. Select the day(s) and time to run the task.
 - a. Click the box next to the day(s) to select the day.
 - b. Click the down arrows and select the hour, minutes, and AM or PM from the drop-down list for each day.
 - c. To enter days/times more quickly, select **Set Multiple Days** to set multiple days with the same time.
 - d. To remove all settings, click **Clear All**.
10. A **Repetitive Task** is one that you schedule to start on a given day, at a certain time, for the number of times you specify, such as every 10 days starting today. The repetition rate can be set to any number of minutes, hours, or days.
 - a. Enter the **Repetition Rate** using whole numbers.



A repetition rate of zero causes the task to run only once.

- b. Click the down arrow and select **Minutes**, **Hours**, or **Days** from the drop-down list.

- c. Enter the date and time for the task to run in the **Next Scheduled Time** field using the format MM/DD/YY hh:mm AM/PM Time Zone.
- d. Click **Update** to update the **Next Scheduled Time** field or change the **Repetition Rate**.



The new Repetition Rate does not take effect immediately. It starts the next time the scheduled task runs. For the new Repetition Rate take effect immediately, click **Update**.

11. Click **OK**.

Actions

Actions	Group Type	Description
Certificate Expiration Monitor	None	Generates a warning, critical warning, and expiration events for the certificates listed in Certificate Management. See Certificate management on page 828
Custom Script	None	Executes the selected command line script located in /home/cm/scripts.
Database Archive and Purge	None	Archives and purges Event, Connection, and Alarm records that are older than 7 days. The number of days is configurable in the Event And Alarm Age Time field on the FortiNAC Properties window. See Database archive on page 977 .
Database Backup	None	Back up the FortiNAC database. The database backup files are stored on the local appliance at /bsc/campusMgr/master_loader/mysql/backup. See Remote backup configuration on page 986 for more information on configuring backups to a remote server.
Disable Adapters	Hosts	Prohibits network access to all adapters in the associated host group. Disables the adapters but not the host itself.
Disable HP/NT Port Security	Devices	Disables port security configuration on all HP/NT devices in the associated group. Use Port Security to disable hosts if DeadEnd VLANs are not used on the network.
Disable Ports	Port	Administratively disables all ports in the associated group.
Enable Adapters	Hosts	Allows network access to all hosts in the associated group.
Enable HP/NT Port Security	Devices	Enables port security configuration on all HP/NT devices in the associated group. Use Port Security to disable hosts if DeadEnd VLANs are not used on the network.

Actions	Group Type	Description
Enable Ports	Port	Administratively enables all ports in the associated group.
Modify Device VLAN Values	Ports	Writes the indicated VLAN value to the switch and changes only the Current VLAN value in the FortiNAC device model. You must specify the VLAN value.
Purge Remediation Output Files (Reports)	None	Purges the output files from all the Nessus scans performed since the last purge.  Nessus Servers and scans are no longer supported.
Resynchronize Device	Devices	Allows you to sync a device with FortiNAC after making a change to the device (e.g., adding a VLAN, role or SSID for a wireless device).
Role Assignment	Hosts	Modifies the Role for the associated group of hosts or users. You must specify the new role.
SSID Assignment	Devices	Maps VLAN IDs to SSIDs. You must specify the both the VLAN ID and the SSID.
System Backup	None	Back up the FortiNAC system files. The system backup files are stored on the local appliance at <code>/bsc/backups/<server name></code> See System backups on page 990.
Update Default VLAN Values	Ports	Sets the Default VLAN value for the port in FortiNAC device model to the value entered in the scheduled task. You must specify the VLAN value.
Update Interface Status	Devices	Reads and updates the interface status for each port on the devices in the associated groups.
Update Remediation Center	None	Connects to Nessus.org and updates the Nessus server with the scan IDs for the version running on the application server. Also connects to Fortinet and updates the server with the latest scan profiles.  If you create scan profiles with Nessus Wx, you must run this task to ensure that those scan profiles will work properly.  Nessus Servers and scans are no longer supported.

Add other scheduled tasks

Tasks can be added to the Scheduler in two ways. You can go directly to the scheduler and create a new task for a group. Certain tasks can only be created from other configuration windows. For example, to schedule a weekly update of your Auto-Def file you must go to the Auto-Def Update window. This task is created and displays on the Scheduler window, but it cannot be created within the Scheduler window. The table below describes scheduled tasks that are created outside the Scheduler window, but, once created, display within that window.

Task	Definition
Scan	Scans that are part of Endpoint Compliance Policies for hosts can be set to run at regular intervals. See Schedule a scan on page 556 .
Proactive Scanning	Security Policy schedules are affected by Proactive Scanning.
Report Generation	Schedule reports to be automatically generated. See Schedule reports on page 802 .
Auto Definition Synchronizer	Weekly updates to your Auto-Def file can be scheduled.
Synchronize Users From Directory	Schedule your LDAP or Active Directory to synchronize with your user database. See Schedule synchronization on page 879 .
Security Rescan	Schedule your scanned host list to be cleared so that Admin scans can begin again. See Clear scanned hosts list on page 618 .
Verify DHCP Servers	Schedule a poll for rogue DHCP servers. See Rogue DHCP server detection on page 892 .

Copy a task

1. Select **System > Scheduler**.
2. Use the filters to display a list of tasks.
3. Click the task to select it.
4. Click **Copy**.
5. Enter a name for the new task.
6. Modify other fields as needed.
7. Click **OK**.
8. The new task appears in the **Scheduler**.

Delete a task

1. Select **System > Scheduler**.
2. Use the filters to display a list of tasks.
3. Click the task to select it.
4. Click **Delete**.
5. Click **Yes** to delete the task.

Modify a task

You can change a task from a Repetitive task to a Fixed Day task by changing the task's date, time, and repetition rate. You can also change the group associated with the task and the name of the task. For Settings see [Add a task on page 858](#).

1. Select **System > Scheduler**.
2. Use the filters to display a list of tasks.
3. Click the task to select it.
4. Click **Modify**.
5. Modify the data as needed.
6. Click **OK**.

Run task now

To run a scheduled action at any time:

1. Select **System > Scheduler**.
2. Use the filters to display a list of tasks.
3. Click the task to select it.
4. Click **Run Now**.

Tasks

Any assigned, active tasks will appear in the top-right corner of the FortiNAC page under a new bell notification icon. Each task has a message, an icon to present who it's assigned to (either you, or everyone), and a pencil with which to edit the task. Some tasks may optionally also have a redirect icon which can be clicked to take you to a different view within the site. At the bottom of this notification drop-down, there is a cog menu to click for Task Settings (which for now is only to show tasks you've assigned).

Aside from this notification panel, there is a main Task view which you can navigate to via the left navigation pane under **System > Tasks**. Here you can see and manage all Tasks regardless of assigned or completed states.

The actions you can take are shown via buttons at the top of the page, as well as context menus when right-clicking a task. You can create tasks, edit tasks, mark a task as complete, or delete them altogether.

When creating a new task, the following properties are available to you:

- **Message**: Text to be displayed in the Task List and notification panel.
- **Previous Task (optional)**: A hierarchical feature to link tasks in sequence. The task provided must be completed before the task being created/edited can be completed.
- **Associated View (optional)**: A view within the navigation which will be opened when the user clicks Open View
- **Assignee (optional)**: A user to assign this task to. If left blank, the task will be assigned to everyone
- **Note (optional)**: Added text field for more robust information; only viewable from the Task view, not the notification panel.

Settings

The settings view provides access to global system configuration options, such as Aging properties to remove hosts and users from the database or email settings for emailing users and administrators.

All settings can also be unified under **System** by enabling **Unified Settings** under **System > Feature Visibility**.

Users & Hosts Setting	Description
User/Host Management	
Aging	Configure default settings to age users and hosts out of the database. See Aging on page 1006 .
Allowed Hosts	Configure the default number of hosts that can be registered to a user. See Allowed hosts on page 1008 .
Device Profiler	Enable or Disable creating rogues from DHCP packets heard on the network. See Device profiler on page 1008 .
MAC Address Exclusion	Lists the MAC addresses that can be ignored by FortiNAC when they connect to the network. These addresses will not be treated as rogues and will be allowed on the production network. See MAC address exclusion on page 1009 .
Network Setting	Description
Authentication	
LDAP	Directories on page 868
Roaming Guests	Roaming guests on page 901
Control	
Access Point Management	Provides the ability to manage hosts connected to hubs using DHCP as a means to control or restrict host access. See Access point management on page 905 .
Allowed Domains	Specify the domains and production DNS server that isolated hosts use to gain access to network locations. See Allowed domains on page 907 .
Quarantine	When quarantine VLAN Switching is set to Enable and the ports are in the Forced Remediation Group, FortiNAC switches unregistered hosts that are being scanned to the quarantine VLAN until the scan process is completed. See Quarantine on page 908 .
Identification	

Network Setting	Description
Device Types	Displays icons representing each device type in the system, and allows you to add, modify, and delete custom type icons.
NAT Detection	Enter the IP ranges where FortiNAC will allow NAT'd hosts. IP addresses outside this range could be NAT'd hosts and can generate an event and an alarm to notify the network administrator. See NAT detection on page 888 .
Rogue DHCP Server Detection	Monitors approved DHCP servers operation and detects rogue DHCP servers on the network using a dedicated interface on the FortiNAC appliance. It defines a scheduled task to run and search specific VLANs and discover all active entities serving IP addresses. This task compares the discovered DHCP servers against a list of authorized DHCP servers and triggers corresponding events when there is no match. See Rogue DHCP server detection on page 892 .
Vendor OUIs	Allows you to modify the vendor OUI database, which is used to determine whether or not a MAC address is valid or by device profiler to profile devices by OUI. The database is updated periodically through the Auto Definition update process. See Vendor OUIs on page 898 .
Network Device	
Network Device	Set global properties that are specific to network devices and VLANs. See Network device on page 910 .

System Setting	Description
Reports	
Analytics	Configure the connection between the FortiNAC server and the cloud reporting Analytics server. This connection allows an agent on the FortiNAC server to push data for reporting to an external server based on a user-defined schedule.
Persistent Agent	
Agent Update	Enable Persistent Agent updates by operating system, schedule agent updates and add hosts to the list of Update Exceptions. You can update agents on both platforms simultaneously or separately. See Agent update on page 913
Credential Configuration	Configure how credentials are verified for hosts who use the Persistent Agent. See Credential configuration on page 918 .
Properties	Configure the FortiNAC server name of the server for Persistent Agent communication, enable or disable display notifications to the host, configure Header and footer text for the Persistent Agent authentication page and Status messages in the message box on the user's desktop. See Properties on page 919 .
Status Notifications	Configure how users are notified of their host status when the Persistent Agent contacts the FortiNAC server.

System Setting	Description
	See Status notifications on page 924 .
Transport Configuration	Configure TCP and UDP communication between the FortiNAC server and the Persistent Agent. See Transport configurations on page 926
USB Detection	Use the USB Detection view allows to configure FortiNAC to be notified in the event that a USB device was plugged into a host on the network. See USB detection on page 929 .
System Communication	
Addresses	Configure a list of address and address group objects used in SSO and VPN configuration. See Addresses on page 935 .
Email Settings	Enter settings for your email server. This allows FortiNAC to send email to Administrators and network users. See Email settings on page 937 .
Firewall Tags	Configure Logical Network Firewall Tags
Fortinet FSSO Settings	Enable FortiNAC as a Fortinet Fabric Connector. For details see the FortiNAC Security Fabric / SSO integration guide .
Log Receivers	Configure a list of servers to receive event and alarm messages from FortiNAC. See Log receivers on page 938 .
Email/SMS Message Templates	Customization of SMS and E-Mail messages for Self-Registered and Pre-Registered Guests
Mobile Providers	Displays the default set of Mobile Providers included in the database. FortiNAC uses the Mobile Providers list to send SMS messages to guests and administrators. The list can be modified as needed. See Mobile providers on page 1 .
Patch Management	The Patch Management feature allows integration with Patch servers such as BigFix or PatchLink. See Patch management on page 940 .
Proxy Settings	Configure FortiNAC to direct web traffic to a proxy server in order to download OS updates and auto-definition updates.
SNMP	Set the SNMP protocol for devices that query FortiNAC for information. It is also used to set the SNMP protocol to accept SNMPv3 traps that register hosts and users. See SNMP on page 948 .
Syslog Files	Syslog Files that you create and store are used by FortiNAC to parse the information received from these external devices and generate an event. The event can contain any or all of the fields contained in the syslog output and can be mapped to an Alarm and an Alarm action. See Syslog files on page 963 and Map events to alarms on page 784 .

System Setting	Description
Trap MIB Files	Enter configurations to interpret SNMP trap MIB information sent from a device and associate it with events and alarms in FortiNAC. See Trap MIB files on page 973 and Map events to alarms on page 784 .
System Management	
Database Archive	Set the age time for archived data files and configure the schedule for the Archive and Purge task. See Database archive on page 977 .
Database Backup/Restore	Schedule database backups, configure how many days to store local backups, and restore a database backup. Note that this restores backups on the FortiNAC server, not backups on a remote server. See Database backup/restore on page 980 .
High Availability	Configuration for Primary and Secondary appliances for high availability. Saving changes to these settings restarts both the Primary and Secondary servers. See High availability on page 981 .
License Management	View or modify the license key for this server or an associated Application server. See License management on page 983 .
NTP And Time Zone	Reset the time zone and NTP server for your FortiNAC appliances. Typically the time zone and NTP server are configured using the Configuration Wizard during the initial FortiNAC set up. Requires a server restart to take effect. See NTP and time zone on page 985 .
Power Management	Reboot or power off the FortiNAC server. See Power management on page 986 .
Remote Backup Configuration	Configure Scheduled Backups to use a remote server via FTP and/or SSH. See Remote backup configuration on page 986 .
System Backups	Create a backup of all system files that are used to configure FortiNAC. See System backups on page 990 .
Updates	
Agent Packages	Displays a list of the Dissolvable Agent, Persistent Agent, and Passive Agent versions available on your FortiNAC appliance. Download new agents and add them to FortiNAC as they become available from Fortinet using Download . Download an Administrative template for GPO configuration to your PC from the FortiNAC appliance using the links at the top of the view. See Agent packages on page 992 .
System	Use System Updates to configure download settings, download updates from Fortinet, install updates and view the updates log. See Agent updates on page 1001 .

Authentication

Authentication groups together options to configure the connection to authenticate using a Google account, to configure an LDAP directory to authenticate users, to configure RADIUS servers to authenticate users, and to configure a list of local domains for your local network users.

Enabling authentication allows the Administrator to determine whether or not hosts connecting to the network will be forced to authenticate. Hosts can be forced to reauthenticate after a specified period of time.

Once a host is registered the host connecting via a wired connection may or may not have to authenticate depending on what port is being used. Hosts connecting via a wireless connection will be forced to authenticate if an authentication VLAN has been established. See [Wireless integration](#) for more information.

Switches used in the forced authentication process must have a value entered for the authentication VLAN in the model configuration. The ports on these switches must be added to the forced authentication group. See [Groups on page 843](#) for details on adding ports to a group.

Options

Option	Definition
LDAP	Use LDAP to configure the connection to one or more authentication directories. Data from the directory populates the FortiNAC database with demographic data for registered users. See Directories on page 868 .
Roaming Guests	Use roaming guests to configure a list of local domains for your local network users. Users who connect and attempt to authenticate with a fully qualified domain name that is not on this list are treated as roaming guests. Applies only to wireless 802.1x connections. See Roaming guests on page 901 .

Automatic authentication

Hosts can be automatically authenticated during registration. This requires the use of either the Dissolvable Agent or Persistent Agent. For details on the agents see the and [Using the Persistent Agent on page 501](#) sections.

Dissolvable Agent

1. Enable authentication. See [Add or modify a policy on page 481](#) for details.
2. When the host downloads and runs the Dissolvable Agent, the host is automatically authenticated.

Persistent Agent

1. Enable authentication. See [Add or modify a policy on page 481](#) for details.
2. When the host downloads and installs the Persistent Agent, the host is automatically authenticated.

Directories

Use the authentication directories view to configure the connection with one or more LDAP directories. If you plan to use local authentication via the FortiNAC database or RADIUS authentication then this step is not necessary.

A directory is a database that contains the records of an organization's members. You can organize the members into groups within the directory. If configured in FortiNAC the directory can be used to authenticate network users. If you have chosen LDAP authentication in the portal configuration window, you must configure a directory in FortiNAC. See [Portal configuration on page 631](#) or [Configure authentication credentials on page 737](#).

The directory configuration validates the user and populates the user record in the FortiNAC databases with user-specific information before they are allowed access to the network. FortiNAC uses the LDAP protocol to communicate to an organization's directory.

A user's record is made up of fields that contain information about the user such as first name, last name, and email address. The name of a field in a directory is defined by a schema. For example, the schema specifies that a user's first name is stored in a field with an attribute name of "givenName". This attribute name is used when retrieving a user's first name from the record. Attribute names can vary from directory to directory, so FortiNAC allows you to define your own fields. Users in an "ou" in the directory are populated into a group in FortiNAC if the distinguished name (DN) attribute is entered in the directory group attribute mappings view.

When an administrator group is created in FortiNAC with the same name as a group being synchronized from a directory, the administrator group members will remain the same as the directory group members. Therefore, if you add a non-directory user to the administrator group and then synchronize the directory, the non-directory user is removed from the administrator group because the user is not a member of the directory group.

Authenticate using a domain name

If you chose to authenticate using a domain name, you must consider the following:

- When a domain name is specified and the login includes the matching domain, authentication first uses both the user name and the domain name. If this authentication fails, no further authentications are attempted.
- When a domain name is specified and the login includes a domain that does not match, the authentication immediately fails.
- When no domain is specified and the login includes a domain, authentication first uses the user name and the domain name. If this authentication fails, a second authentication is attempted using only the user name.
- Domain names must be an exact match. For example, if you define the domain as example.com, a login of john.smith@it.example.com is not authenticated because the domain specified is not an exact match.
- The table below provides a summary of the various formats which FortiNAC uses to interpret the fully qualified username and to identify the user portion (which can sometimes be a host), the domain portion and the separator.

Fully qualified username	User	Domain
user	user	no domain specified
user@domain.com	user	domain.com
user@domain	user	domain
domain\user	user	domain
domain.com\user	user	domain.com

Authenticate using domain names and multiple directories

If you are using multiple directories to authenticate users, you must consider the following:

- When one directory is configured and no domain is specified, authentication is attempted using the one directory.
- When multiple directories are configured and no domain is specified, authentication is attempted to all directories that are in the database. The order in which the directories are processed cannot be controlled, and the first directory that yields a successful authentication is used. Therefore, if settings such as Security & Access Attribute Value, Role, etc., are not identical between all configured directories, a user's network access can vary based on which directory settings are in effect. These settings will depend on the most recent directory sync.
- When multiple directories are configured, authentication is attempted against all directories without Domain configurations, or with Domain configurations matching the domain, if one is supplied. If a Domain is configured for the directory, the user must supply a matching value for their domain in order for authentication to be attempted to that directory.
- If duplicate user Id's are present within the directories then the Identifier attribute mappings must contain unique values. Use userPrincipalName or mail attributes. Using sAMAccountName only recommended for the default directory without a Domain Name configured all others must provide a unique user ID value.

Note: Domain Name can be a semi-colon separated list in the following format. EXAMPLE;example.com

Requirements

The following steps provide a basic outline for the procedures required to setup the directory and its communication with FortiNAC.

1. Enable ping on the directory server itself. This allows FortiNAC to ping the directory server and prevents the server Icon in the Network Device Summary panel on the dashboard from displaying an error as if it had lost contact when, in fact, it is in contact via LDAP.
If you plan to use the top level (root) of the directory tree as a Group search branch, make sure that you use Config Wizard to configure DNS in FortiNAC so that the IP address of the directory can be resolved to the directory's hostname. In addition, the IP address must be resolved by the primary DNS server.
2. Set up the connection between the directory application and FortiNAC. This step provides login information allowing FortiNAC to connect and communicate with the directory. See [Configuration on page 870](#).
3. Map directory data fields to FortiNAC data fields. This step allows you to import user and group information into your database.
4. Configure User and Group Search Branches.
5. Data in your directory can change frequently. Users could be added, removed or modified. Those changes need to be incorporated into your FortiNAC database. Create a schedule to synchronize the directory with the FortiNAC database. See [Schedule synchronization on page 879](#).
6. If choosing to use SSL or TLS security protocols for communications with the LDAP directory:
 - TLS 1.2 or TLS 1.3 must be enabled on the LDAP directory
 - Installing a security certificate isn't necessary in most cases. However, if needed, see [Create a keystore for SSL or TLS on page 881](#).
7. If you choose to use logon/logoff scripts to register the host when a user logs on or off a domain.

You may need to access your directory using a separate interface to acquire login, group and user information.

If you create new users in the directory, be sure not to assign a user ID that is the same as an existing user account or guest account in the FortiNAC database. Having duplicate user IDs will prevent one or both of the users from accessing the network.

Structure and synchronization

When synchronizing FortiNAC with a directory there are specific configuration tasks that must be completed. FortiNAC does not have a view into the structure of your directory; however, you must understand this structure to complete the configuration.

You may have your own application to view the attributes of your directory or there are some available on the Internet, such as Active Directory Explorer, LDAP Administrator, or Apache Directory.

Configuration

Directory configuration allows you to configure the connection to the directory, user attributes that you would like to import, user search branches and Group Search Branches. Each configuration section has specific information that must be entered to allow FortiNAC to connect with the directory and import users and groups.

Use **Schedule** to configure the intervals for synchronizing the database with the selected directory. Use **Preview** to review data in the selected directory. Use **Copy** to copy the directory configuration fields from an existing configuration.

Directory configuration can be accessed from **System > Settings > Authentication > LDAP**.

Connection tab

The Connection tab contains the parameters required for communication with the directory. Not all fields are required. Be sure to enter information only in those fields that apply to your directory.

Settings

Field	Description
Name	Name of the server where the directory is hosted.
Primary IP	IP address of the primary directory server. The server will be added as a pingable device.
Security Protocol	The security protocol used when communicating with the server containing your directory. Options are SSL, STARTTLS, and none. If SSL or STARTTLS are chosen you must have a security certificate from a CA. The certificate should be stored in the following directory on your appliance <code>/bsc/campusMgr/</code> See Create a keystore for SSL or TLS on page 881 for instructions on importing and storing certificates.
MAC address	Physical address of the primary directory server. This field is required.
LDAP Login	User login name of the service account FortiNAC uses to access the LDAP server. Service account must have read access to all requested search branches.
LDAP Password	Password for the user login.
Validate Credentials	Click to verify that directory credentials are correct.

Field	Description
Credential Status	Displays the results of clicking Validate Credentials . Messages such as credentials verified or failed to validate can be displayed.
Additional Configuration	Displays the fields listed below in this table.
Domain Name	If this field contains a domain name, users must include the domain name in their login to be authenticated against this directory. Example: Valid formats for login are: user, user@domain.com and domain\user. Setting a value here requires all users to supply a domain name during login. When no domain is specified in the Directory Configuration view and the login includes a domain, authentication first uses the user name and the domain name. If this authentication fails, a second authentication is attempted using only the user name.
Secondary Server	FQDN or IP address of the secondary directory server. This server would be accessed in the event that the Primary server was unavailable. This server is added as a pingable device. Important: Value must be FQDN if Security Protocol = SSL or STARTTLS. Note: FortiNAC uses the same LDAP Login and Password to contact both directories.
Version	Directory version. Default = 3
Port	Communication port used by the directory. The default port is based on the security protocol. To use a port other than the default, type the desired port number into this field. Common port values/protocols are: • None = 389 • SSL = 636 • STARTTLS = 389
Time Limit	Time in seconds that FortiNAC waits for a response from the directory. Default = 5. The number of seconds may need to be increased in the directory or in FortiNAC if the exception "Time Limit Exceeded" begins to be noted more often.
Enable Synchronization of Users/Groups At Scheduled Time	Check this box to synchronize the FortiNAC database with either the primary or the secondary directory servers based on a schedule in the Scheduler View.
on sync, delete Users no longer found in this directory	When checked, users that have been removed from the directory will be removed from the FortiNAC database when the scheduled resynchronization takes place.
Perform Lookup On Referral	Referrals allow administrators to set up search paths for collecting results from multiple servers. If you have configured your directory for referrals and you want to do authentication on the referred directory servers, enable this option. Enabling referrals is required in order to search sub domains.
Connect by Name	Automatically checked when StartTLS is selected as the Security Protocol.

Field	Description
	FortiNAC connects to LDAP using the the Name field of the directory configuration with a URL such as ldap://dc.example.com to connect to the primary server. When not selected, FortiNAC will connect to LDAP using the Primary IP address field of the directory configuration with a URL such as ldap://10.0.0.2.
NetBIOS name	When specified, authentication will be via Kerberos. This represents the domain NetBIOS name of the active directory server. This must match a domain NetBIOS name from one of the configured Winbind instances in Network > RADIUS > Winbind.

The Administrator must enter the specific connection information for the directory server used for user authentication. The Security information required varies depending on the type of directory you are using. Be sure to enter only the data required for your directory type.

The Directories View can be accessed either from **System > Settings > Authentication > LDAP**.

1. Click **System > Settings**.
2. Click the **Authentication** folder in the tree control.
3. Click **LDAP** to display the Directories window.
4. To Modify a directory, select a directory in the list and click **Modify**.
5. To Add a directory, click **Add**.
6. A list of directories found on your network is displayed. Click on the name of the directory to be added. If the directory is not listed, click **Enter Manually**. Directories are found based on SRV records on your corporate DNS.
7. Use the information in the Settings table above to enter connection information.
8. Click the **Connection** tab and enter connection information.
9. Click **Validate Credentials** to verify the connection.
10. If FortiNAC is able to successfully connect to the directory a **Credentials Verified** message is displayed in the Credential Status field.
11. To ensure that the user data is available to FortiNAC, you must also complete the User Attributes, Group Attributes, Search Branches and Select Groups tabs.
12. Click **Next** to continue.

User attributes tab

To add users from an LDAP compliant directory, the customer user database schema must be mapped to the FortiNAC user data. Attributes can be mapped for users and groups by selecting the tabs on the left side of the window.

If a user in the directory has multiple attributes with the same attribute ID, FortiNAC uses the first one it finds. For example, if a record looked like the one shown below, FortiNAC would use staff.

```
eduPersonalAffiliation=staff
eduPersonalAffiliation=employee
eduPersonalAffiliation=alum
eduPersonalAffiliation=student
```

The attribute mappings for the user are entered on the User Attributes Tab. The AD attributes are mapped on this form for User Description, Contact, Hardware, and Security and Access. This allows FortiNAC to retrieve the user information based on the User Search Branches configured on the Search Branches tab.

Configure user attributes

When adding a directory FortiNAC attempts to determine the directory type and populates the attribute fields based on the directory type. Do not modify the directory type unless it is incorrect. Do not modify the attributes unless they are incorrect.

The value of an attribute being mapped cannot exceed 255 characters in order for the attribute to be retrieved by FortiNAC.

1. To access user attributes for an existing directory, select **System > Settings**.
2. Click the **Authentication** folder in the tree control.
3. Click **LDAP** to display the directories window.
4. If you are **adding a new directory**, the **User Attributes** tab is displayed when you click **Next** after completing the connection tab.
5. The **Directory Type** drop-down indicates the type of directory being configured. This will scan the directory based on the type selected and pre-populate some of the fields. The directory type should already be listed for you. If the directory type is not listed or you know the field names for your directory, this step is not required.
6. Enter the user attribute mappings.
7. The Identifier (ID) field is a required entry. User records in the directory must have data entered in the selected ID field.
Note: As of version 8.7.0, the Last Name is no longer a required field.
8. To ensure that the user data is available to FortiNAC, you must also complete the **Group Attributes**, **Search Branches**, and **Select Groups** tabs.
9. Click **Next** to continue.

Directory attributes

If you are using Active Directory, keep in mind that Active Directory only allows access via LDAP to users whose primary group is the Domain Users group.

User attributes	Active Directory	Novell
Object Class	user	person
Description		
First Name	givenName	givenName
Last Name *	sn	sn
Identifier *	sAMAccountName	cn
Title	title	
E-mail	userPrincipalName	
Contact		
Address	streetAddress	mailstop
City	l	city
State	st	S
Zip/Postal Code	postalCode	

User attributes	Active Directory	Novell
Phone	telephoneNumber	Telephone Number
Mobile Phone	mobile	
Mobile Provider	otherMobile	
	 The provider contained in the Mobile Provider field in the directory must match a provider in the FortiNAC database or SMS messages cannot be sent to that user's Mobile phone. Depending on the configuration of your directory, otherMobile may not be the location of the Mobile Provider field.	
Security and access		
Security Attribute	The Directory Attribute that can be used in a filter. Data contained in this field is copied to the Security and Access value field on the User Properties and the Host Properties record for each user and associated host when the directory synchronizes with the database.	
Allowed Hosts	The number of host records each individual user may have in FortiNAC.	
Role	Name of the Directory Attribute used to associate a user with a role.  Matching roles must be created in FortiNAC with the exact same spelling and case as the roles that exist in the directory based on the selected attribute. See Roles view on page 625. When assigning roles to users, the use of directory attributes over directory groups is recommended. Under no circumstances should you use both methods to assign roles.	
Disabled Attribute	Setting this attribute allows the AD Administrator to disable users in Active Directory and have all instances of the user automatically disabled in FortiNAC when the next scheduled resync occurs. Attribute = <code>userAccountControl</code>	

User attributes	Active Directory	Novell
	 Disabled users are able to access the network until FortiNAC resynchronizes with the Active Directory. To immediately disable all instances of the user in FortiNAC, go the Scheduler View and run the Synchronize Members with Directory task. See Scheduler on page 857 for more information.	
Disabled Value	When the value for the Disabled Attribute for the user equals the Disabled Value, FortiNAC disables all instances of a user when the next scheduled resync with AD occurs. The user must have previously been disabled in AD. The Disabled Value may vary from directory to directory. Check a user that is currently disabled in the directory to see what the disabled value should be. Enter that value in the Disabled Value field. If "Disabled Value" starts with a "0x", a bitwise comparison is done between the value in the directory and this field. Otherwise, without the "0x" prefix, it will only do an exact match numeric comparison.  If you are using Active Directory, it is possible for the Disabled Value to vary from user to user. The value is affected by other account settings selected within the directory, such as Password Never Expires or User Must Change Password At Next Login. You may only be able to set the Disabled Value for users that have identical account settings. See https://support.microsoft.com/en-us/kb/305144 for more information on these values.	
Time To Live	The name of the directory attribute that contains the numerical value for the user age time. If the attribute does not have a value the user age time is not set by the directory. Age time can also be set using the Properties window or on the User Properties window for an individual user. All of these options simply modify the Expiration Date in the User Properties window. See User properties on page 200.	

User attributes	Active Directory	Novell
	 The value of the attribute in the Time To Live field must be set to the name of the custom attribute that is configured in the directory as the numerical value of hours or days for which the user is valid.	
Time to Live Unit	The time unit set in the User Properties age time if the Time to Live attribute contains a value. Options: Hours or Days	

Group attributes tab

The attribute mappings for groups are entered on the Group Tab. The AD attributes are mapped on this form for Object Class, Group Name and Members. This allows FortiNAC to retrieve the group information based on the Group Search Branch configured on the Search Branches Tab. Groups created in the directory are imported into FortiNAC each time the Directory Synchronization task is run either manually or by the Scheduler.



Active Directory size limitations for the number of users per group may cause issues with group based operations. Only the users up to the limitation are affected by group based operations. Size limitations vary depending on the version of Active Directory used and the settings in the MaxValRange and MaxPageSize directory fields.



The value of an attribute being mapped cannot exceed 255 characters in order for the attribute to be retrieved by FortiNAC.

Configure group attributes

1. To access group attributes for an existing directory, select **System > Settings**.
2. Click the **Authentication** folder in the tree control.
3. Click **LDAP** to display the directories.
4. If you are adding a new directory, the **Group Attributes** tab is displayed when you click **Next** after completing the User Attributes tab.
5. Enter the group attribute mappings:

Group Attributes	Active Directory	Novell
Object Class	group	groupOfMembers
Group Name	name	cn
Group Members	member	member
Distinguished Name (DN)		



The DN is not to be used in conjunction with groups identified by Object Class.

6. To ensure that the user data is available to FortiNAC, you must also complete the Search Branches and Select Groups tabs.
7. Click **Next** to continue.

Search branches tab

The Search Branches tab is where the Administrator enters the specific User and Group Search Branches information for the Directory server. This tells FortiNAC where the user and group information is located in the Directory.



Active Directory size limitations for the number of users per group may cause issues with group based operations. Only the users up to the limitation are affected by group based operations. Size limitations vary depending on the version of Active Directory used and the settings in the MaxValRange and MaxPageSize directory fields.

The example shown in the figure below is for Active Directory. In this example the segments represent the following:

cn=Users: The abbreviation cn stands for Common Name. In this case, it is the name of the branch or folder in Active Directory that should be searched for users. The name of that branch could be anything, such as Employees or Students.

dc=example: The abbreviation dc stands for Domain Component. In this case it is the second level domain name, such as yahoo in yahoo.com.

dc=com: The abbreviation dc stands for Domain Component. In this case it is the first level domain name, such as com in google.com or edu in marshalluniversity.edu or org in npr.org.

Configure search branches

1. To access search branches for an existing Directory, select **System > Settings**.
2. Click the **Authentication** folder in the tree control.
3. Click **LDAP** to display the directories.
4. To modify an entry, select the **entry** and click **Modify**.
5. To remove an entry, select the **entry** to be removed and click **Delete**.
6. If you are adding a new directory, the **Search Branches** tab is displayed when you click **Next** after completing the **Group Attributes** tab.
7. Click **Add** to add new search branch information. Available search branches are listed; however you can enter your own information. If the list of available search branches is too long to display, type the first few letters of the branch needed to narrow the list.
8. In the Add dialog, enter or select the **Search Branch** and then click **OK**.
9. To ensure that the user data is available to FortiNAC, you must also complete the Select Groups tab.
10. Click **Next** to save search branch information.

Select groups tab

Use the Select Groups tab to choose groups of users to be included when the directory and the FortiNAC database are synchronized. Upon initial synchronization, a host group and a user group are created for each LDAP group selected. Hosts become members of these groups when they are registered to a user that is a member of that LDAP group. **Note:** If a group with the same name already exists, a host group will not be created.

Users that do not already exist in FortiNAC are not imported. However, user data for users already in the database is updated each time the Synchronization task is run. Only the members of selected groups will be synced (put in the groups) and not ignored for syncing the attributes.

Configure group selections

1. To access group selections for an existing directory, select **System > Settings**.
2. Click the **Authentication** folder in the tree control.
3. Click **LDAP** to display the directories.
4. If you are adding a new directory, the **Select Groups** tab is displayed when you click **Next** after completing the **Search Branches** tab.
5. Mark the groups of users that should be included when the directory and the database are synchronized by checking the box in the **Active** column. If you do not check any boxes, all groups will be included.
6. Select from the dropdown list to filter the Group inside this branch. **Note:** The search bar only supports regex (*) wildcard matching.
7. Click **OK** to save the directory configuration.
8. An initial Synchronization is done immediately when you save the Directory. It is recommended that you set up a schedule for synchronizing the Directory See [Schedule synchronization on page 879](#).

Select OU tab

Use the Select OU tab to choose groups of users to be included when the directory and the FortiNAC database are synchronized. Upon initial synchronization, a host group and a user group are created for each LDAP group selected. Hosts become members of these OUs when they are registered to a user that is a member of that LDAP OU. **Note:** If a group with the same name already exists, a host group will not be created.

Users that do not already exist in FortiNAC are not imported. However, user data for users already in the database is updated each time the Synchronization task is run. Only the members of selected OUs will be synced (put in the OUs) and not ignored for syncing the attributes.

Configure OU selections

1. To access OU selections for an existing directory, select **System > Settings**.
2. Click the **Authentication** folder in the tree control.
3. Click **LDAP** to display the directories.
4. If you are adding a new directory, the **Select OU** tab is displayed when you click **Next** after completing the **Search Branches** tab.
5. Mark the groups of users that should be included when the directory and the database are synchronized by checking the box in the **Active** column. If you do not check any boxes, all groups will be included.
6. Select from the dropdown list to filter the OU inside this branch. **Note:** The search bar only supports regex (*) wildcard matching.

7. Click **OK** to save the directory configuration.
8. An initial Synchronization is done immediately when you save the Directory. It is recommended that you set up a schedule for synchronizing the Directory See [Schedule synchronization on page 879](#).

Delete a directory

1. Click **System > Settings**.
2. Click the **Authentication** folder in the tree control.
3. Click **LDAP** to display the Directories window.
4. Select a directory configuration in the list and click **Delete**.
5. Confirm that you wish to delete the directory configuration.

Replace a directory

If replacing an existing directory with another directory, use the following steps. Otherwise, some user records may remain associated to the old directory. See related KB article [209296](#) for details:

1. Delete the old directory. See steps above.
2. Add the new directory using the old directory name.
3. Modify the LDAP directory and change the old directory name to the new directory name.
4. Select **OK**. This re-writes the name attribute to all of the user records and can take a few minutes.
5. Run the Synchronize Members with Directory task from the Scheduler view. See [Run task](#) now for instructions.

Schedule synchronization

When you select **Schedule** on the **Directories** view, you can select a date/time and poll interval for the directory synchronization task. The scheduled task may also be paused and run manually later. This process adds the **Synchronize Members with Directory** task to the scheduler.

When the directory and FortiNAC are synchronized, changes made to users in the directory are written to corresponding user records in the database. Users from the directory are only added to the FortiNAC database when they connect to the network and register.

FortiNAC supports Machine Authentication with RBAC based on compute groups in the Active Directory (AD). This feature was introduced in FortiNAC version F 7.6.0. Upon initial synchronization, FortiNAC now creates 2 groups for each directory group:

- Host group renamed as <directory group name>_host
- User group renamed as <directory group name>_user

Note: FortiNAC does not create groups based upon the directory primary groups at this time.

If the directory group contains registered machines, those machines will be added to the new host group.

If the directory group contains users already in the FortiNAC database (due to user authentication or machine authentication), those users will be added to the new user group.

Example:

Directory group "Lab" has that following:

5 machines (3 are registered in FortiNAC)

8 users (4 accounts are present in FortiNAC database due to user authentication or machine authentication)

After initial synchronization, FortiNAC creates 2 groups:

Lab_host with 3 hosts

Lab_user with 4 users

Specific directory groups can be disabled from attribute mappings. See **Select groups** tab under configuration for details. If an Administrator group with the same name already exists, a host group will not be created. Any new groups created in the directory are detected upon the following synchronization. Groups created are displayed in FortiNAC on the Groups View.

If you are using a directory for authentication, user data is updated from the directory based on the user ID during synchronization. This is true regardless of how the user is created and whether the user is locally authenticated or authenticated through the directory. If the user ID on the user record matches a user ID in the directory, the FortiNAC database is updated with the directory data.

When an administrator group is created in FortiNAC with the same name as a group being synchronized from a directory, the administrator group members will remain the same as the directory group members. Any group membership changes made in the directory group are updated in FortiNAC's administrator group upon the next synchronization.

The directory schedule is global and applies to all directories listed. Separate schedules cannot be entered for each directory.

Settings

Field	Definition
Schedule Interval	Poll interval for the scheduled task. Options are Minutes, Hours, or Days.
Next Scheduled Time	The next date/time the scheduled synchronization task will run. Entered in the format MM/DD/YY HH:MM AM/PM.
Enabled	When unselected, the scheduled synchronization task is stopped and does not run automatically. To run the task manually click Run Now.
Run Now	Runs the Synchronization task immediately.

Schedule directory resynchronization

1. Click **System > Settings**.
2. Click the **Authentication** folder in the tree control.
3. Click **LDAP** to display the Directories window.
4. Select a directory in the list and click **Schedule**.
5. Set a **Schedule Interval** by entering a number and selecting Minutes, Hours, or Days from the drop-down menu.
6. Click in the **Next Scheduled Time** field and enter the **date/time** to run the synchronization task.
7. To stop the scheduled task, remove the check mark from click in the **Enabled** box.
If the scheduled task is disabled, the Administrator can go to the Scheduler view and run the task manually to synchronize the directory with FortiNAC. See [Scheduler on page 857](#) for details.
8. To run the scheduled task immediately, click **Run Now**.
9. Click **OK** to save the schedule.

Preview

Use **Preview** to view the list of users that are found in the directory. User records in the directory are not listed until a parameter is selected and its associated value is entered in the **Filter** field.

The directory configuration must be completed before any records can be previewed.

1. Click **System > Settings**.
2. Click the **Authentication** folder in the tree control.
3. Click **LDAP** to display the Directories window.
4. Select a directory in the list and click **Preview**.
5. Enter search criteria in the first text field, such as an ID or Last Name. Searches are not case-sensitive.
Use asterisks (*) as wild cards in text fields if you know only a portion of a name. The wild card represents any characters. For example, enter F* in the text field and select the First Name parameter to locate all records where F is the first character in the First Name field.
6. Select a **parameter** from the drop-down list.
7. Click **Search**.

An asterisk in the **Role** column next to an attribute value indicates that the role name has not been configured in FortiNAC. If the role does exist in FortiNAC, the attribute value appears in the Role column without an asterisk.

Entering just the wild card in the text field returns every record in the directory and may cause time or size limit exceeded errors to occur depending on the total number of records.

This is a view only list and is not imported into FortiNAC. The user information is only imported into the FortiNAC database as the user registers. The **Sync Directory** task in the **Scheduler** is used to update user information already in the FortiNAC database with any changes made in the directory database. See [Scheduler on page 857](#) for additional information.

8. Click the **Groups** tab to view the groups in the directory and select the groups to import.
All the groups in the directory are listed along with the number of member records contained in each group.
Selecting groups is part of the process of adding a directory configuration, therefore, groups may already be selected.
9. **To import groups** of user records from the directory to the FortiNAC database when the directory Synchronization scheduled task runs select the groups to be imported by checking the box(es) next to the group name.
10. A check mark in the **Is Organizational Unit** column indicates that the group is an OU or a container for other groups.
11. Click **OK**.

Create a keystore for SSL or TLS

When using SSL or TLS security protocols for communications between FortiNAC and some servers (such as LDAP directory, Fortinet EMS and Nozomi servers) a security certificate may be required. The need for the certificate is dependent upon the configuration of the directory. In most cases, FortiNAC automatically imports the certificate it needs. However, if this is not the case, use the following steps to import the certificate.

Certificate Import Instructions:

1. Once the certificate from the CA has been received, login to the FortiNAC server CLI as root.
Note: If using NAC-OS, login to CLI as admin then run:
`execute enter-shell`
2. Copy the file to the `/home/admin` directory.

3. Use the keytool command to import the certificate into a keystore file.
keytool -import -trustcacerts -alias ldap_client -file /home/admin/MainCertificate.der -keystore .keystore
Example using certificate file named MainCertificate.der:
keytool -import -trustcacerts -alias ldap_client -file MainCertificate.der -keystore .keystore
For additional information on using the keytool key and certificate management tool go to the Sun web site java.sun.com.
4. When the script responds with the **Trust this certificate?** prompt, type **Yes** and press **Enter**.
5. At the prompt for the keystore password, type in the following password and press **Enter** `^8Bradford%23`
6. To view the certificate, navigate to the `/home/admin` directory and type the following:
keytool -list -v -keystore .keystore
7. Type the password used to import the certificate and press **Enter**.
8. Verify connection to the directory. In the Administration UI, navigate to **System > Settings > Authentication > LDAP**.
9. Double click the directory model and click the **Validate Credentials** button.

If unable to connect, restart the FortiNAC control process to clear any cached information:

1. In the FortiNAC CLI, type:
`sudo shutdownCampusMgr`
2. Wait 30 seconds
3. Type:
`sudo startupCampusMgr`

Identification

Identification groups together methods of detecting and identifying rogue hosts. Options include:

Option	Definition
Device Types	Displays icons representing each device type in the system, and allows you to add, modify, and delete custom device type icons.
NAT Detection	Lists the IP ranges where FortiNAC Manager will allow NAT'd hosts. IP addresses outside this range could be NAT'd hosts and can generate an event and an alarm to notify the network administrator. See NAT detection .
Rogue DHCP Server Detection	Monitors approved DHCP servers operation and detects rogue DHCP servers on the network using a dedicated interface on the FortiNAC Manager appliance. It defines a scheduled task to run and search specific VLANs and discover all active entities serving IP addresses. This task compares the discovered DHCP servers against a list of authorized DHCP servers and triggers corresponding events when there is no match. See Rogue DHCP server detection .
Vendor OUIs	Allows you to modify the vendor OUI database, which is used to determine whether or not a MAC address is valid or by device profiler to profile devices by OUI. The database is updated periodically through the Auto Definition update process. See Vendor OUIs on page 898 .

Device types

Add and modify and see which device types are in use.

Starting with version F 7.6.3, FortiNAC has expanded its device detection database by integrating FortiGuard Category and Subcategory mappings. This enhancement brings improved classification and identification of connected devices, aligning FortiNAC more closely with FortiGuard's comprehensive IoT detection capabilities.

Previously, FortiNAC supported only 27 predefined device types. With this update, a broader range of device types is now supported, leveraging FortiGuard's taxonomy, which includes over 120 subcategories.

As a result, FortiNAC can now detect and classify over 140 distinct device types. This expansion retains all previously supported device types, ensuring backward compatibility while significantly improving visibility and control across diverse device environments.

With the updated device type database in version 7.6.3, the expanded device type list is reflected throughout the FortiNAC interface.

- On the Host page, the Device Type column displays updated values based on the enhanced classification set. Same in the Device Type column in Adapters page and the Type column in Profiled Device page.
- In Vendor OUI Settings, the Registration Type Override dropdown includes the newly added device types, allowing more precise control over registration behavior based on MAC address vendor mappings.
- Similarly, when adding a new Device Profiling Rule, the Type selection now reflects the full list of supported device types, enabling more accurate profiling and policy assignment.

Please refer to the end of the page for a full list of expanded device types.

To access the Device Type View, select **System > Settings > Identification > Device Types**.

Add a New Device Type

1. Click **Add**.
2. Define a **Name** for the new Device Type.
3. Either upload the device type icons from your local computer, or select **Select from Archive** to use archived icons from FortiNAC.
4. Click OK to save.

Modify a Device Type

1. Select a device type and click **Edit**.
2. Edit the device type information.
3. Click **OK** to save.

Delete a Device Type

System Defined Device Types cannot be deleted.

1. Select a added Device Type from Admin, click **Delete**.
2. A confirmation message is displayed. Click **Yes** to delete the Device Type.

Device Type in Use

1. Select one **Device Type**.
2. Click **In Use**.

The pop up window displays the objects currently using the selected device type.

Full List of System Defined Device Types

- Alarm
- Alarm System
- Android
- AP
- Apple iOS
- Appliance
- Arduino
- Audio Player
- Automotive
- Baby Monitor
- Barcode Scanner
- Blood Analyzer
- Cable Box
- Camera
- Card Reader
- Circuit Board
- Cleaner
- Clock

- Cloud
- Communication
- Computer
- Conferencing
- Controller
- Database
- Dental Chair
- Dental Device
- Desktop
- Diagnostic & Screening
- Dialup Server
- Disc Player
- Doorbell
- Electric
- Energy
- Environmental Control
- Ereader
- File Server
- Firewall
- Fitness
- Fridge
- Game Console
- Gaming Device
- Garage Door
- Gateway
- Generic
- Generic Monitoring System
- Health Care Device
- Health Monitor
- Hub
- Human Machine Interface
- HVAC
- Implants & Prosthesis
- Industrial Device
- IP Camera
- IP Phone
- Ipod
- IPS/IDS
- Laboratory
- Laptop
- Light
- Linux
- Lock

- MacOS
- Mail Server
- Media
- Media Player
- Medical Device
- Meter
- Microphone
- Mobile Device
- Modem
- Motion Detector
- NAS
- Network
- Network Appliance
- Neurology & Cardiology
- Patient Monitoring
- PBX
- PCoIP Endpoint
- PDU
- Pet Monitor
- Phone
- Photo Camera
- Photo Display
- Pingable
- Plug
- PoE Switch
- Point of Sale
- Pool
- Power System
- Printer
- Processing Unit
- Programmable Logic Controller
- Projector
- Radio
- Raspberry
- Registered Host
- Remote Control
- RFID Tag
- Robot
- Router
- Satellite
- Scale
- Scanner
- Security System

- Sensor
- Server
- Sleep Tech
- Small Cell
- Smart Device
- Smart Home
- Smoke Detector
- Solar Panel
- Sound System
- Speaker
- Sprinkler
- Sterilization Equipment
- Storage
- Surgery
- Switch
- Tablet
- Television
- Terminal
- Thermostat
- Touch Panel
- Toy
- Unix
- UPS
- USB
- Vending Machine
- Virtual Machine
- Voice Control
- VoIP Device
- VPN
- VR
- Washer
- Watch
- Water Sensor
- Wearable
- Weather
- Web Server
- Wifi Extender
- Windows
- Wireless Access Point

NAT detection

A NATing device is a device (e.g., a router) that sits on your network and performs Network Address Translation (NAT) to share network resources with one or more devices behind the NATing device. This could be a security risk to your network. An administrator can see the NATing device by its IP; however, the other devices behind it remain hidden.

NAT Detection has the ability to identify the following:

- A host/device that has a NIC card with an IP that does not match the IP address of the device connected directly to the port.
- A user is MAC spoofing, where the user registers the host and then sets the NATing device's MAC address to the host's MAC address

The key to NAT detection is identifying the authorized IP ranges (i.e., for Production, Remediation etc.). The Dissolvable Agent or Persistent Agent gathers host IP and MAC address information. The NAT device will be within the authorized range, but the host behind it is served an IP by the NAT device and its IP is outside the range. This mismatch triggers events and alarms that indicate that a NATing device is being used.

The information gathered by the agent is returned to the FortiNAC server and analyzed as follows:

- FortiNAC determines whether or not the IP address of the device connected directly to the port is within the range specified for NAT detection.
- If the IP address is within the NAT detection range, then FortiNAC verifies that one of the IP addresses returned by the Agent matches the IP address of the device connected directly to the port. The agent can only return the IP addresses of the host, not the NAT device. If none of the IP addresses of the host sent match the IP address of the device on the port, then a "Possible NAT User" event is generated.



If a network user sets local or self-signed IP addresses on the host that is behind the NAT device, no event is triggered.

- The agent also returns the MAC addresses of the interfaces on the host. If FortiNAC detects that the device connected to the port and the interfaces on the host have the same MAC address, it generates a "Possible NAT Device, MAC Spoofed" event.

By mapping alarms to notify management when these events occur, you can identify and remove NATing devices from your network.

If you want to allow a router with hosts connected behind it to access your network, you must enable NAT Detection by entering the IP ranges within which using a NAT device is permitted and detected. If NAT Detection is not enabled, or the router is given an IP address that is not within a NAT detection range, both the router and the host behind it are left in registration. The administrator is not notified that a NAT device is connected.

To run NAT Detection, the following requirements must be met:

- Hosts must use either the Dissolvable Agent or the Persistent Agent
- At least one security policy must be defined to use the Dissolvable Agent or Persistent Agent
- Designate the IP address ranges that FortiNAC should monitor.
- Map the NAT detection events to alarms with an appropriate action (e.g., notify management). See [Map events to alarms on page 784](#) for details.



If you have a host trying to connect through a router, and that router is not in an IP address range being checked for NAT Detection, that host will be stuck in Registration. Create IP address Ranges in NAT Detection that encompass any of IP address the router could be given.

Add or modify IP ranges

You must enter a separate range of IP addresses for each subnet.

Example:

Range 1 = 192.168.5.2 - 192.168.5.255

Range 2 = 192.168.6.2 - 192.168.6.255

Do not enter a single range spanning both of the above 192.168.5.2 - 192.168.6.255

1. Click **System > Settings**.
2. Expand the **Identification** folder and click **NAT Detection**.
3. Click **Add**.
4. Enter the starting and ending IP addresses for the range and click **Add**.
5. Repeat for additional ranges of IP addresses.

Remove an IP range

1. Click **System > Settings**.
2. Expand the **Identification** folder and click **NAT Detection**.
3. Select an IP range to be deleted.
4. Click **Delete**.

NAT detection configurations and results

NAT detection configuration and corresponding results can be complex. Below are a series of examples detailing common scenarios and the results shown in FortiNAC.



The IP addresses used in the examples below are only for illustration purposes. They are not the specific IP addresses you will see on your own network.

For the purposes of the examples assume the following:

- Network IP Range for Production = 10.10.5.50 - 10.10.5.99
- Network IP Range for Registration = 10.10.5.100 - 10.10.5.200
- NAT Detection has been configured with the following IP ranges:
 - 10.10.5.50 - 10.10.5.99
 - 10.10.5.100 - 10.10.5.200

Scenario 1: NAT detection enabled, using endpoint compliance policy and agent

1. The user connects a router to a port on your network and then connects a host to the router.
2. Neither the router nor the host are registered.
3. The router is placed in Registration and is given a Registration IP address of 10.10.5.101. The host is given IP address 192.168.1.1 by the router.
4. The user goes through the registration process and is assigned an endpoint compliance policy.



NAT Detection requires that the host have an agent installed.

5. The IP address of the router is within one of the IP ranges set up for NAT Detection. The IP address of the host is sent by the agent to FortiNAC. FortiNAC determines that the host IP address is outside the IP ranges set up for NAT Detection. This process triggers a "NAT Device Registered" event.
6. When the host itself is registered a "Possible NAT User" event is triggered.
7. On the **Host View**, the router has been registered as a NAT Device to the user. The router has an IP address in the Production range, such as 10.10.5.51. The Registered To field displays User Name - NAT Device, such as Doe, John - NAT Device. The Host icon is displayed and shows as on-line.
8. On the **Host View**, the PC behind the router is registered as a host to the user. The Host's IP address displays as a production IP address, such as 10.10.5.50. However, the host actually still has the IP served by the router of 192.168.1.1. The Registered To field displays only the user name, such as Doe, John. The Host icon is displayed and shows as offline even though the host is on-line.

Scenario 2: NAT detection enabled, not using endpoint compliance policy or agent

1. The user connects a router to a port on your network and then connects a host to the router.
2. Neither the router nor the host are registered.
3. The router is placed in Registration and is given a Registration IP address of 10.10.5.101. The host is given IP address 192.168.1.1 by the router.
4. The user goes through the registration process.
5. On the **Host View**, the router has been registered as a PC to the user. The host connected to the router is not shown because FortiNAC is unaware of the host's existence behind the router.
6. Events associated with a NAT device are not generated.
7. Eventually the router is moved to Production and the host can access the network and the Internet. This may require the user to release and renew the IP address on the router by disconnecting and reconnecting the router to the port.

Scenario 3: NAT detection disabled, not using endpoint compliance policy or agent

1. The user connects a router to a port on your network and then connects a host to the router.
2. Neither the router nor the host are registered.
3. The router is placed in Registration and is given a Registration IP address of 10.10.5.101. The host is given IP address 192.168.1.1 by the router.
4. The user goes through the Registration process, but there is no endpoint compliance policy required. The user does not download an agent.
5. The only IP address information provided to FortiNAC is the information returned from the switch where the router is connected when it is polled.

6. The router is assigned a Production IP address, such as 10.10.5.55.
7. The host behind the router continues to use the 192.168.1.1 IP address assigned by the router.
8. On the Host View, the router has been registered to the user, but FortiNAC is unaware that this device is a NAT Device. The Registered To field displays User Name, such as Doe, John . The Host icon is displayed and shows as on-line.
9. FortiNAC is not aware of the host behind the router, therefore, its information is not displayed. The user of this host can access the network and the Internet.
10. In this scenario the user may need to release/renew the IP address on both the host and the router to access the Internet.

Scenario 4: NAT detection disabled, using endpoint compliance policy and agent

1. The user connects a router to a port on your network and then connects a host to the router.
2. Neither the router nor the host are registered.
3. The router is placed in Registration and is given a Registration IP address of 10.10.5.101. The host is given IP address 192.168.1.1 by the router.
4. The user goes through the Registration process and is assigned an endpoint compliance policy which includes downloading and installing either the Dissolvable Agent or the Persistent Agent.
5. The router is not registered and is trapped in the registration VLAN. The host is registered but is also trapped in the registration VLAN because it is connected to the router.
6. In the Host View, the router continues to display as a rogue. The host is registered but shows as offline.

Docking Station Management

Overview

Docking Station Management provides secure oversight of devices connected through docking station or Ethernet dongle by identifying them via their MAC addresses. While docking stations enable various devices to access the network using the station's MAC address, this can inadvertently allow untrusted devices to connect to sensitive resources. Docking Station Management is specifically designed to mitigate this risk by ensuring that only authorized devices gain access, thereby preventing unwanted or unauthorized connections through docking stations.

How it Works?

When a device connects to the network via a docking station, an authentication policy is enforced to verify its legitimacy. The system checks whether the device is registered in the Docking Station Management list. If the device is not recognized, it is automatically placed into an authentication VLAN. From there, the user is directed to a self-registration portal, where they must authenticate the device before gaining access to the network.

Device MAC Address Management

☰

🔍

⚙️ Authentication >

⚙️ Control >

⚙️ Identification ✓

Device Types

NAT Detection

Docking Station Management

Rogue DHCP Server Detection

Vendor OUIs

Network Device

⚙️ Persistent Agent >

⚙️ System Communication >

⚙️ System Management >

⚙️ Updates >

⚙️ User/Host Management >

+ Add New

📄 Import CSV

✎ Edit/View

🗑 Delete

📤 Export ▾

⋮ More ▾

🔍 Search

MAC Address	Last Modified By	Last Modified Time
00:50:56:B5:FB:BE	admin	2025/09/17 14:15:26

Action	Description
Add New	Add a device MAC address to the list of devices that connect through docking station. Re-authentication through VLAN will not be necessary through this method.
Import CSV	Import a list of device MAC addresses that connects through the docking station. Re-authentication will not be needed when the list of MAC addresses are added through this method.
Edit/View	Edit or view the device MAC address that connects through the docking station.
Delete	Delete the selected device MAC address that connects through the docking station.
Export	Export the list of device MAC addresses that connect through docking station in CSV format.

Rogue DHCP server detection

Rogue DHCP Detection monitors approved DHCP servers operation and detects rogue DHCP servers on the network. This feature uses a dedicated interface on the FortiNAC appliance. It defines a scheduled task to run and search specific VLANs and discover all active entities serving IP addresses. When the Rogue DHCP Detection task runs, it will switch the port designated as the System DHCP Port to each of the VLANs designated. During the switch to each VLAN,

the port admin state is set to down then back to up after the configuration to the new VLAN ID. This task compares the discovered DHCP servers against a list of authorized DHCP servers and triggers corresponding events when there is no match. These are suspected unauthorized DHCP servers and are managed according to the alarms that are mapped to the events.

Requirements

- FortiNAC must be configured for L2 Network Type. For details on this network type, see [Configuration Wizard guide](#)
- A dedicated network interface on FortiNAC. Installation of an additional Network Card may be required.
- IP address for the dedicated network interface. This should be an unused IP address from an unused subnet on the network. Configure the IP address through the CLI by modifying the `vlanInterfaces` file in `/bsc/siteConfiguration`. If unfamiliar with this file, contact Customer Support for assistance.

Implementation

- The Authorized DHCP Servers must be added to the Authorized DHCP Servers group.
- The DHCP Port must be indicated in the System DHCP Port group.
- Polling VLANs for Rogue DHCP servers must be scheduled.



If IP Helper is being utilized on the network an additional configuration step will be required to make FortiNAC aware of the Authorized DHCP Servers.

Rogue DHCP events and alarms

Event	Definition
Rogue Host DHCP Server Application	A host is serving IP addresses (i.e., a DHCP response was seen from a host).
Rogue Device DHCP Server Application	A device is serving IP addresses.

These events can be mapped to alarms. Alarms can be set to notify an administrator when they are triggered. Alarms can also be viewed on the Alarms Panel in the dashboard. For more information on events and alarms, e-mail notifications, SMS notifications, and how to map events to alarms see [Map events to alarms on page 784](#).

Configure an IP address for a new interface



To modify an IP address for the port1 or port2 interface, use the Configuration Wizard.

To add an IP to an interface (other than the port1 and port2 interface), add an entry to the appropriate interface in the `vlanInterfaces` file and run the `network restart` command as follows:

1. Access the CLI on the FortiNAC Server or Application Server.
2. Navigate to the `siteConfiguration` directory.

```
cd /bsc/siteConfiguration
```
3. Edit the `vlanInterfaces` file.
4. Add the new IP address to the appropriate interface. The following example adds `IPADDR_1` to `eth2`:

```
ifcfg-eth2|IPADDR='188.11.32.2', NETMASK='255.255.255.0', STARTMODE='onboot', BOOTPROTO='static',  
IPADDR_1='188.11.32.3', NETMASK_1='255.255.255.0', LABEL_1='1'
```
5. Run the following command(s).

```
service bsc-network start  
service network restart
```

Server detection configuration

Rogue DHCP Server Detection Configuration allows you to indicate which interface on the appliance is used for scanning VLANs. The interface used varies depending on the configuration of your FortiNAC environment.

All FortiNAC appliances

The `port1` interface is always used for management and cannot be used for rogue DHCP detection.

FortiNAC Server

On a FortiNAC, `port2` is typically used for the captive portal, leaving `eth2` for Rogue DHCP Server Detection.

FortiNAC Control Server/Application Server Pair

On a FortiNAC Application Server and FortiNAC Control Server pair, the captive portal is typically on `port2` on the Application Server. You could use `port2` on the Control Server for Rogue DHCP Server Detection. You may need to add a network card to your server to provide an interface for Rogue DHCP Server Detection.

Once you have determined the interface to use for Rogue DHCP Server Detection, it must be configured with an IP address. The IP address should be an unused address from an unused subnet on your network. To configure the IP address go to the CLI on the server and modify the `vlanInterfaces` file in `/bsc/siteConfiguration`. When the interface has been configured, enter it on this view.



If you are using Rogue DHCP Server Detection in a high availability environment, both the primary and secondary servers must have the same Interface setting. In addition, the ports to which the Interfaces connect must be added to the System DHCP Port group. See [Modify a group on page 846](#) for details.

In the event of a failover, it is important that these fields be setup correctly or DHCP monitoring will not run.

Settings

Field	Definition
Interface	Ethernet interface used by the FortiNAC appliance for Rogue DHCP Server Configuration, such as eth2.
Authorized DHCP Servers	Device group containing the list of servers that are authorized to serve DHCP. The Authorized DHCP Servers group can be modified here or on the Groups View.
System DHCP Ports	Port group containing the port where the FortiNAC interface is connected to the network. The System DHCP Ports group can be modified here or on the Groups View.
VLANs To Scan For Rogue DHCP Servers	ID and Name of the VLANs that should be scanned for Rogue DHCP servers. If a VLAN is not entered in the list, it is not scanned for Rogue DHCP servers. Only the VLANs entered here are scanned.
Schedule DHCP Server Verification	Use a scheduled task to set the poll interval and scheduled time to poll the selected VLANs for rogue DHCP servers.

Configure server detection

1. Click **System > Settings**.
2. Expand the **Identification** folder.
3. Select **Rogue DHCP Server Detection** from the tree.
4. In the **Interface** field enter the ethernet interface used by the FortiNAC appliance for Rogue DHCP Server Configuration.
5. Click **Modify** next to **Authorized DHCP Servers** to add the servers that are allowed to serve DHCP into the Authorized DHCP Server group.
6. On the Modify Group dialog click the **Container** where the servers are located to expand the list. Mark each server with a check mark and click the right arrow in the center of the screen to move the selected servers to the Selected Members column.
7. Click **OK** to save the changes to the group.
8. Click **Modify** next to **System DHCP Ports** to update the System DHCP Ports group with the port where the FortiNAC interface is connected to the network.
9. On the Modify Group dialog click the **Container** where the switch is located.
10. Click the switch where the FortiNAC Rogue DHCP Detection Server interface is connected. A list of the ports on the selected switch appears below the switch.



Select the switch and port where the FortiNAC network card is connected, such as port2 or eth2. This is the connection that will handle the scanning for Rogue DHCP Servers. Do NOT select the DHCP Server itself or the port the DHCP Server is connected to. Do NOT select the switch or port where the FortiNAC port1 network card is connected.

11. Select the **Port** where the Rogue DHCP Detection server is connected and click the right arrow to move the port to the Selected Members column.
12. Click **OK** to save the changes to the group.
13. In the **VLANs To Scan For Rogue DHCP Servers** section, click **Add**.
14. In the **Add** dialog enter the ID and Name of the VLANs that should be scanned for Rogue DHCP servers and click

OK.



If a VLAN is not entered in the list, it is not scanned for Rogue DHCP servers. Only the VLANs entered here are scanned.

15. Click **Save Settings**.

Schedule DHCP server verification

Use the Schedule option to set the poll interval and scheduled time to poll the selected VLANs for rogue DHCP servers.

1. Click **System > Settings**.
2. Expand the **Identification** folder.
3. Select **Rogue DHCP Server Detection** from the tree.
4. Click **Modify Schedule**.
5. Select the **Enabled** check box.
6. Enter a name for the task in the Name field.
7. The **Description** field is optional. Enter a description of the task.
8. Action type and Action are pre-configured based on the task and cannot be modified.
9. From the **Schedule Type** drop down list, select either **Fixed Day** or **Repetitive** and set the day and time that the task is to be performed.
10. A **Fixed Day Task** is one in which you schedule a task to run on a combination of days of the week and times of the day, such as Mondays at 1:00 pm and Fridays at 10:00 am. Select the day(s) and time to run the task.
 - a. Click the **box** next to the day(s) to select the day.
 - b. Click the **down arrows** and select the hour, minutes, and AM or PM from the drop-down list for each day.
 - c. To enter days/times more quickly, select **Set Multiple Days** to set multiple days with the same time.
 - d. To remove all settings, click **Clear All**.
11. A **Repetitive Task** is one that you schedule to start on a given day, at a certain time, for the number of times you specify, such as every 10 days starting today. The repetition rate can be set to any number of minutes, hours, or days.
 - a. Enter the **Repetition Rate** using whole numbers.



A repetition rate of zero causes the task to run only once.

- b. Click the **down arrow** and select **Minutes**, **Hours**, or **Days** from the drop-down list.
- c. Enter the **date and time** for the task to run in the **Next Scheduled Time** field using the format MM/DD/YY hh:mm AM/PM Time Zone.



The new Repetition Rate does not take effect immediately. It starts the next time the scheduled task runs. For the new Repetition Rate take effect immediately, click **Update**.

- d. Click **Update** to update the **Next Scheduled Time** field or change the **Repetition Rate**.

12. Click **OK**.
13. Click **Save Settings**.

Schedule settings

Field	Definition
Remove local backups older than	Number of days for which you would like to keep backups. Anything older than the number of days entered, is removed the next time the scheduled task for backups runs. This setting removes backup files created on the FortiNAC server before they are copied to the remote server. Backups on the remote server are not removed. The timing of the scheduled backup task and the age of the files that are to be removed must be thought out carefully or you will remove all of your backups. For example, if the remove option is set to 5 days and your backup task runs every 15 days, you may inadvertently remove all of your backups. However, if the remove option is set to 15 days and the backup task runs every 5 days, then you would always have backup files.
Status	Indicates whether the task is enabled or disabled.
Schedule Interval	How often the scheduled task runs.
Next Scheduled Time	The next date and time the scheduled synchronization task will run. Entered in the format MM/DD/YY HH:MM AM/PM
Modify Schedule	Allows you to modify the scheduled activity.
Run Now	Runs the scheduled task immediately.

Rogue DHCP server detection with IP helper

When IP Helper is in use, an IP address for the Authorized DHCP Server is returned to FortiNAC for each VLAN. This IP address has a MAC address associated with it. FortiNAC compares the IP address it receives with the list of valid Authorized DHCP Server IP addresses. If the FortiNAC list does not contain the IP and the related MAC address, it does not recognize the DHCP Server as authorized.

The following procedure must be completed to enable FortiNAC to recognize the returned Authorized DHCP Server IP addresses as valid.

1. Create a Pingable model in the Inventory for each IP Helper Address.
 - a. In the Inventory, click the container where devices are located.
 - b. Right-click and select **Add Pingable Device**.
 - c. Enter the **Device Name**, **IP address**, **Protocol** (set to Pingable), and select the **Device Type** of Pingable.
 - d. Click **Apply**.
2. Ensure that the Pingable model has a MAC address.
 - a. Click the **Pingable model** in the Inventory to select it.
 - b. Right-click and select **Properties**.
 - c. Enter the **MAC address** associated with the IP address.
 - d. Click **Apply**.
 - e. Close the **Device Properties** window.

3. Place the Pingable model in the Authorized DHCP Server group.
 - a. Select **System > Groups**.
 - b. Click the **Authorized DHCP Servers** group to select it.
 - c. Right-click and select **Modify**.
 - d. Click the container where the Pingable models were created. A list of the devices in the container will be displayed in the below the container.
 - e. Click the **Pingable model(s)** to mark them with a check mark.
 - f. Click the right arrow to move your selections to the **Selected Members** column.
 - g. Click **OK**.
 - h. Select **System > Groups** and click **Show Members** and verify that all the pingable models are listed.

Vendor OUIs

Use the vendor OUI database to determine whether a particular MAC is valid. As new IEEE device information becomes available, the database needs to be updated to reflect the new codes. This prevents **invalid physical address** errors when devices with the new MACs are connected to the network. The AutoDef Synchronization scheduled task automatically updates the vendor OUI database. See [Scheduler on page 857](#) for additional information on scheduling tasks.

You can search the vendor OUI database, and add, modify, or remove vendor OUIs. Vendor OUI Added and vendor OUI Removed events are generated when you add or remove vendor OUIs.

The vendor name appears in the Host View unless you enter a vendor OUI alias. If you use a vendor OUI alias to identify the type of device, you can quickly filter all devices with a specific alias. For example, you can manage gaming devices by adding the vendor OUI to the database with the vendor OUI alias of **Gaming Device**. Then you can use the Host View filter to find these records by name, change them to registered, and assign them a role without requiring the device to be assigned to a user.

Vendor OUIs are also used with the device profiler feature. Device profiling rules can use the vendor OUI to help identify rogue devices connecting the network. Depending on the instructions associated with the rule, the device can be automatically assigned a device type and be placed in the Host View, the Inventory or both. See [Profiled devices on page 251](#) for additional information.

To access the vendor OUI View select **System > Settings > Identification > Vendor OUIs**.

Add a vendor OUI

1. Click **System > Settings**.
2. Expand the **Identification** folder and click **Vendor OUIs**.
3. Click **Add** at the bottom of the window.
4. Use the table below to enter the vendor OUI information:

Field	Description
Vendor OUI	First 3 octets of a device's Physical Address. Enter in the hexadecimal format ##:##:## (For example, 00:1D:09)
Vendor Name	Name of the vendor that owns the vendor OUI.

Field	Description
Vendor Alias	Value entered displays as the host name in the Host View. This field is optional when adding a vendor OUI.
Role	Role for devices associated with this vendor OUI. Roles assigned by device profiler take precedence. If a device is registered via the Portal Page, then the role associated with the vendor OUI is applied. See Roles on page 620.
Registration Type	Type of device registration that is specified through the AutoDef Synchronization update, such as a Camera, a Card Reader or a Gaming Device. In the Add/Modify vendor Code dialog the current setting for the vendor code Registration Type is displayed. Options include Manual or a specific device type.
Registration Type Override	Used to specify a Registration Type that is different from the default supplied by the AutoDef Synchronization update. Options include Manual or a specific device type.
Description	User specified description of the vendor OUI.
Last Modified By	User name of the last user to modify the vendor OUI.
Last Modified Date	Date and time of the last modification to this vendor OUI.
Right click options	
Delete	Deletes the selected vendor OUI.
Modify	Opens the Modify Vendor OUI dialog.
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746.
 You must have permission to view the admin auditing log. See Add an administrator profile on page 139.	

5. The **Description** field is optional and allows you to add notes about the OUI. This field is not displayed on the vendor OUIs view.
6. Select the **Registration Type Override** for the device.
7. Click **OK**.

Modify a vendor OUI

1. Click **System > Settings**.
2. Expand the **Identification** folder and click **Vendor OUIs**.
3. Search for the appropriate vendor OUI and select it. Click **Modify**.
4. Edit the vendor OUI information
5. The **Description** field is optional.
6. Click **OK**.

Modify multiple vendor OUIs

Multiple vendor OUIs can be modified at the same time to update fields such as Role or Description.

1. Click **System > Settings**.
2. Expand the **Identification** folder and click **Vendor OUIs**.
3. Search for the appropriate vendor OUIs. Select all of the affected vendor OUIs. If they are not part of a continuous list, hold down the CTRL key to select them.
4. Click **Modify**.
5. On the Modify dialog enable the check boxes next to the fields to be updated. Any field that is not enabled will not be affected.
6. Modify the data in the selected fields.
7. Click **OK**.

Delete a vendor OUI

1. Click **System > Settings**.
2. Expand the **Identification** folder and click **Vendor OUIs**.
3. Search for the vendor OUI to be deleted and select it.
4. Click **Delete**.
5. A confirmation message is displayed. Click **Yes** to delete the OUI.

Register devices

To register devices, such as gaming devices, you must enter the vendor OUIs in the vendor OUI database. When the host connects the device to the network a rogue host record is created.

If you are using the device profiler feature, these devices may be processed by a Device Profiling Rule that registers them for you.

1. Enter the vendor OUIs into the database.
2. When entering the vendor OUI be sure to fill in the **Vendor Alias** field. This alias displays on the Host View when a device with this vendor OUI connects to the network.
3. If this device requires a role, select a **Role** on the vendor OUI window. This role is only applied to devices registered manually through the Portal Page.
4. In order to register a device you must make sure that the **Registration Type Override** field in the vendor OUI window is set to reflect the correct device type. For example, if this vendor OUI represents a gaming device, you would select Gaming Device from the list in this field.
5. Once the device is connected to the network, click **Users & Hosts > Hosts**.
6. Locate the record for the rogue device.
7. Select the record. Then, right-click and select **Register As Device**.

Device registration after vendor OUI database update

Devices whose vendor OUIs are not in the database appear in the Host View as rogues when they connect to the network. Once you have entered the vendor OUI in the database, the information in the Host View displays the vendor

OUI data as part of the rogue record. Use the vendor alias to identify the type of device, such as gaming device or security camera, for example. The vendor alias is displayed in the host name column of the Host View.

1. Add the vendor OUI information to the database. Include the vendor alias to aid in grouping the devices.
2. Go to **Users & Hosts > Hosts** and use the filter tabs or column sort features to locate the devices.
3. Select the record(s) and change the device to Registered using the Register As Device option on the right-click menu.

Roaming guests

Use roaming guests to configure a list of local domains for your local network users. Users who connect and attempt to authenticate with a fully qualified domain name that is NOT on this list are treated as roaming guests. This feature was developed to accommodate organizations that meet at each other's sites frequently, such as an educational consortium or a business development group. Supports Eduroam for participating universities.

- For EduRoam configuration, see the [EduRoam Cookbook](#).

This feature can only be used for wireless 802.1x connections.



The hierarchy consists of RADIUS servers at the participating institutions, national RADIUS servers run by the National Roaming Operators and regional top-level RADIUS servers for individual world regions. When a user A, from institution B, in country C with two-letter country-code top-level domain xy, visits institution P in country Q, A's mobile device presents his credentials to the RADIUS server of institution P. That RADIUS server discovers that it is not responsible for the Institution_B.xy realm and proxies the access request to the national RADIUS server of country Q. If C and Q are different countries, it is in turn proxied to the regional top-level RADIUS server, and then to the national RADIUS server of country C, which has a complete list of the participating eduroam institutions in that country. That national server forwards the credentials to the home institution B, where they are verified. The 'acknowledge' travels back over the proxy-hierarchy to the visited institution P and the user is granted access.

RADIUS configuration

Configure your 3rd party RADIUS server local to the site with the remote RADIUS servers to which it should proxy authentication requests for users who are not part of one of your local domains.

Note: The FortiNAC Local RADIUS Server feature introduced in 8.8 does not support the Roaming Guests feature. A 3rd party RADIUS server must be used.

Model configuration

Modify the Model Configuration of any wireless device to which your roaming guests will connect. Specific treatment can be configured for roaming guests in the Model Configuration. This controls network access, such as the VLAN in which the host is placed, or access can be denied for roaming guests on a particular device. See the information for the Host State field in [Model configuration on page 338](#).

Roaming guests cannot be controlled at the SSID level only at the device level.

Local domains

Configure the list of local domains. This allows FortiNAC to distinguish between local users and roaming guests. See Add Local Domains below for instructions.

Notes

- Roaming guests may require a supplicant for the wireless connection. This supplicant cannot be configured by FortiNAC. Easy Connect Supplicant Policies cannot be used for roaming guests because roaming guests are placed in a special network based on the settings in the Model Configuration before the host could be evaluated and assigned a Supplicant Policy.
- Device profiler automatic registration settings are suspended for roaming guests.
- Roaming guests age out of the database in 24 hours.
- If a Roaming Guest logs into a host registered to a local user, the host is treated like a Roaming Guest.
- If a Roaming Guest logs into an existing Roaming Guest host, they are treated as a Roaming Guest.
- If a Roaming Guest has a Persistent Agent installed on their host from their own FortiNAC system, there is no impact on your FortiNAC server.

Connection process

When a Roaming Guest connects to the network, the process is as follows:

1. FortiNAC proxies the request to a local corporate RADIUS server.
2. The local RADIUS server queries the appropriate remote RADIUS server for the domain name contained in the login information. The remote RADIUS servers must be configured within your corporate RADIUS server to allow the authentication request to be proxied to the correct server.
3. The remote RADIUS server replies to the local corporate RADIUS server.
4. That reply is sent to FortiNAC.
5. FortiNAC registers the host in the database as a device and allows the user to connect to the network. The user is shown as a logged in user.
6. Users are placed in a special group called **Roaming Guest Users**.
7. Hosts are placed in a special group called **Roaming Guest Hosts**.

Add local domains

1. Click **Network > Settings > Roaming Guests**
2. Click **Add**.
3. Enter a domain name.
4. Click **OK**.

Multi-factor Authentication

Overview

Multi-factor Authentication (MFA) provides a secondary form of identity verification besides password before granting access to FortiNAC Administrator GUI. MFA prevents unauthorized access and protect FortiNAC from unauthorized user and meet compliance requirement. (GDPR, HIPAA, ISO 27001, etc.)

Types of Multi-Factor Authentication

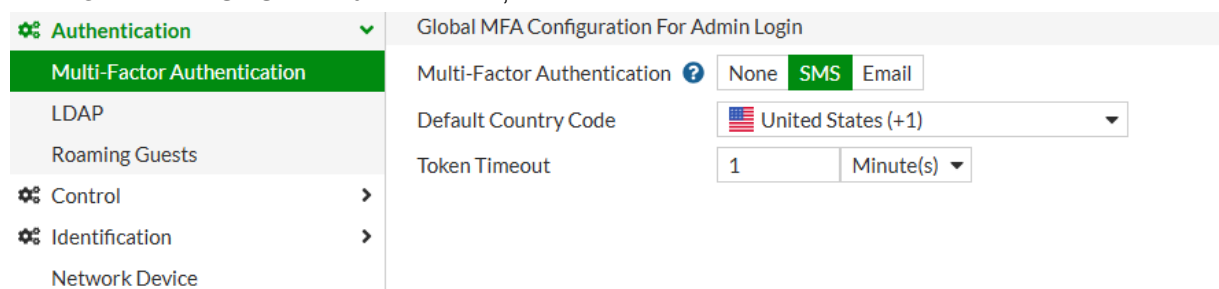
FortiNAC MFA provides two ways to send the one-time token code, either through e-mail or SMS.

There are two types of multi-factor authentication provided by FortiNAC:

1. **Individual MFA** - is accessible through **Users & Hosts > Administrators** page. Click on an administrator and select **Modify** to configure the multi-factor authentication setting.
 - Every administrator has a separate multi-factor authentication setting.
 - If Global MFA is enabled with a default country code, and the administrator hasn't set a personal country code, the system will use the default country code from Global MFA

2. **Global MFA** - is accessible through **System > Settings > Authentication > Multi-Factor Authentication**.

- When Global MFA **SMS** or **Email** is enabled, it enabled multi-factor authentication on all administrators



- **Default Country Code** - When Global SMS is enabled, the default country code will be applied to any administrator who hasn't set a personal country code in their multi-factor authentication settings. If an administrator has already configured a country code, SMS messages will be sent using that administrator's specific country code and phone number
- If the user has a mobile phone number with the corresponding country code, but no mobile provider, Global MFA can still send a SMS through REST SMS Gateway. Please see [REST SMS Gateway Configuration on page 903](#).
- **Token Timeout** - is amount of time given for the token to become invalid for the use of authentication.



Both individual and global MFA can be reset through FortiNAC CLI - execute `admin-ui reset-mfa-settings`. For more information, please see [Execute commands](#) under Admin UI.

REST SMS Gateway Configuration

REST SMS Gateway requires a third-party SMS API to send SMS over FortiNAC REST SMS Gateway.

Setup a third-party SMS API prior to setup a REST SMS Gateway.

Please have setup a third-party SMS API prior to configure the REST SMS Gateway.

1. Go to Network > Service Connectors.
2. Click +Create New and select **REST SMS Gateway** under **Email/SMS**.
3. Fill in the SMS API parameters and click **OK**. Here is an example:

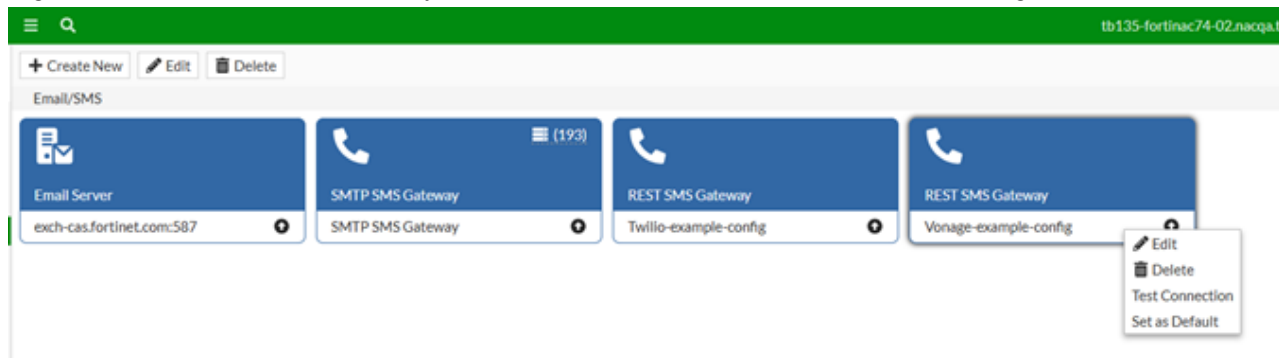
Email/SMS



REST SMS Gateway

Name	Vonage-config
API URL	https://rest.nexmo.com/sms/json
HTTP Method	POST
User Name	
Password	•••••••• Change
Content Type	multipart/form-data
Enabled	☒

4. Right click on the REST SMS Gateway and click **Test connection** to make sure it is working.



5. Right click on the REST SMS Gateway and select **Set as Default** to make it as the default method of sending SMS.

After the setting is completed, any administrator that has a mobile number with a country code but without a mobile provider in the MFA setting will still receive a SMS when attempting to login to FortiNAC.

Control

Control groups together options that determine whether or not hosts can access the network or the internet when they are a rogue or are in remediation. Options include:

Option	Definition
Access Point Management	Manage hosts connected to hubs using DHCP as a means to control or restrict host access. See Access point management on page 905 .
Allowed Domains	Specify the domains and production DNS server that isolated hosts use to gain access to network locations. For example, if hosts are in isolation because they do not have the latest virus definitions for their virus software, they would need to be able to access the web site for their virus software to download virus definitions. See Allowed domains on page 907 .
Quarantine	Globally enables or disables quarantine VLAN switching and allows the administrator to set the risk state for all hosts to safe. See Quarantine on page 908 .

Access point management

Access point management provides the ability to manage hosts connected to hubs using DHCP as a means to control or restrict host access.

If the Access Point (AP) was discovered using device discovery and the AP supports bridging, FortiNAC automatically puts the AP model in the bridging devices group and the interface that the AP is connected to shows up as a link.

For FortiNAC to manage the hosts connecting through the AP the AP must show up connected to an interface of the upstream switch.

Configure an AP

1. Put the port that the AP is connected to into the **Access Point Management** group.
2. Remove the AP from the Bridging Devices group.
3. Undo any uplink setting on the interfaces that the APs are connected to within FortiNAC.
 - a. From **Inventory**, click the device to select it.
 - b. Click the interface that is identified as an uplink to select it, then right-click and select **Port Properties**.
 - c. Turn the User Defined Uplink off, then click Apply.
 - d. Right-click the switch model and select Resync Interfaces.

The link goes away and either the AP or a Cloud is connected to the interface.

This process has to be done for models that were placed in the Bridging Group that have an AP connected. Each interface where an AP is connected on those models needs to be modified so that access point management is applied.

FortiNAC does the following:

- Assigns authorized hosts an IP address from the allocated IP address pool (this allocation is done in the dhcpd.conf file that is updated using the Configuration Wizard)
- Assigns unauthorized hosts an IP address from the allocated IP address pool for all unauthorized hosts (this allocation is done in the dhcpd.conf file that is updated using the Configuration Wizard)
- Updates the DHCP server configuration with authorized IP addresses and the associated MAC address
- Directs authorized hosts to a valid DNS to allow network access
- Directs unauthorized hosts to FortiNAC's access point management DNS
- Verifies whether or not the host accessing the network through an access point has a valid IP address in the DHCP lease file
- Generates a Static-IP-Address event if a host's IP address is not listed in the DHCP lease file maintained by FortiNAC
- Takes action on the Static-IP-Address event when the event is mapped to an alarm and action through the Alarm Mapping functionality

StaticIPAddress event

FortiNAC detects static IP addresses and generates a StaticIPAddress event. When a host connects, FortiNAC checks the DHCP lease file maintained by FortiNAC. If the host's MAC address is in the DHCP lease file, FortiNAC allows the host to connect. If the host's MAC address is not in the DHCP lease file, FortiNAC generates the StaticIPAddress event. You can map this event to an alarm and have action taken on the host. See [Map events to alarms on page 784](#) for details on using this feature.

Configure access point management

Before configuring access point management in FortiNAC make sure that the access point management view with appropriate VLAN ID and IP address ranges has been configured in the Configuration Wizard. See the *Appliance Installation Guide* for directions.

If a host is manually rescanned by selecting rescan on the Host Health tab or an existing scan is manually set to Failed while the host is on the production network, the host remains on the production network until the lease for the IP address expires or the host disconnects from the network. There is no mechanism to move the host to Isolation when it is connected to the network in an access point management environment.

1. Click **System > Settings**.
2. Expand the **Control** folder and click **Access Point Management**.
3. Click the check box next to **Enable Access Point Management**.
4. In the **Configuration Update** field enter the number of seconds that will lapse between updates to the DHCP Configuration file.
5. Click **Add** below the IP address table to add ranges of possible IP addresses. This table only needs to be configured if detecting hosts with Static IP addresses is required.

The IP address ranges entered should include all the possible IP addresses that were made available on the network for access point management when the Configuration Wizard was run.
6. Enter the **Starting** and **Ending IP addresses** of a range of possible IP addresses.
7. Click **OK**.
8. Repeat step 6 through step 8 to enter all the ranges of possible IP addresses.
9. Click **Save Settings** to save all changes to the access point management view.
10. Click **System > Groups** and click the **Access-Point-Management** group to select it.

11. Right-click and select **Modify**.
 12. The All Members panel in the Modify Group dialog displays a list of Inventory containers. Click the + sign next to the container that has the managed switch, and then click the + sign next to the device. Select the port where the access point is connected.
 13. Click the right arrow to move the port to the **Selected Members** column.
 14. Click **OK**.
 15. On the **Groups** view, with the group still selected, click **Show Members** and verify that the port is in the group.
 16. To disable hosts on the access point, set a port on the switch to a secure or static port based on the type of switch in use. This is not the port where the Access Point connects; it is another port on the same switch. See [Secure port/static port overview on page 349](#) for additional information.
- Some switches may require the command line interface rather than the FortiNAC User Interface.

When a Restricted host connects a fake DNS is given. This will resolve to the FortiNAC Application Server DNS.

The Application Server DNS directs to a page which redirects the host to a preconfigured URL, based on host state (At Risk or Unregistered, for example) Registration, Remediation, Quarantine, or Dead End.

Allowed domains

Use the Allowed Domains View to specify the domains and production DNS server that isolated hosts use to gain access to network locations. For example, if hosts are in isolation because they do not have the latest virus definitions for their virus software, they would need to be able to access the web site for their virus software to download virus definitions.

If you have used a valid SSL certificate to secure the portal, add the domain of the CA to the Domains list, such as verisign.com. This allows the host's browser to validate the certificate.

Note: If multiple portals are configured, this list applies to all portals. There is not a separate list per portal.

Field	Definition
IP address	The IP address(es) of the production DNS server(s). If the Prevent the DNS server from making iterative queries check box is enabled, FortiNAC would no longer perform iterative queries to external authoritative servers. If the DNS server does not find the domain, the DNS server will not continue to perform queries to authoritative name servers. The only DNS requests the FortiNAC server will make on behalf of endpoints are to the specified DNS forwarding IPs.
Proxy Auto Config	Optional. If you use a Proxy server, this populates the wpad.dat file with the information that allows a host to learn about the Proxy server. This also adds the Domains listed to allow hosts in Isolation to reach sites related to Anti-Virus or operating system updates required. See Web proxy on page 1 for additional information.
Domains	A list of authorized domains that an isolated host is permitted to access, such as microsoft.com.
Revert To Defaults	Reset the values to the factory settings.

Configure a production DNS server

Enter the IP address(es) of the production DNS server(s) for isolated hosts to have access to network Resources.

1. Select **Network > Settings**.
2. Expand the **Control** folder and click **Allowed Domains**.
3. Click in the **IP address** field and enter the IP address of the production DNS server. Separate multiple IP addresses with a semicolon (;).
4. Click **Save Settings** to save all of your changes.

Add a domain

Wildcards such as * cannot be used when entering Domain names. You can enter a large domain that contains sub-domains. For example, if you enter **Microsoft.com**, users can access all domains for Microsoft. However, if you enter a sub-domain, such as **downloads.microsoft.com**, then users can only access that specific domain.

1. Select **Network > Settings**.
2. Expand the **Control** folder and click **Allowed Domains**.
3. In the **Domains** section of the window, click **Add**.
4. Enter the domain name and click **OK**. Repeat to add additional domains.
5. Click **Save Settings**.

Delete a domain

1. Select **Network > Settings**.
2. Expand the **Control** folder and click **Allowed Domains**.
3. In the **Domains** section of the window, click the domain name to select it.
4. Click **Delete**.
5. Click **Save Settings**.

Revert to the default domains list

To revert to the default list of domains and reset the Production DNS IP address:

1. Select **Network > Settings**.
2. Expand the **Control** folder and click **Allowed Domains**.
3. Click **Revert to Defaults**.
4. Click **Save Settings**.

Quarantine

Quarantine allows the Administrator to set the Risk State for all hosts to Safe. In the event that a scan profile generates significant false negatives which results in multiple hosts being set to At Risk, rather than set each individual host to Safe, this option allows the Administrator to globally change all hosts. Once that has been done, then the scan can be reconfigured and hosts rescanned.

Quarantine VLAN switching can be globally enabled or disabled from the Quarantine view.

1. Click **System > Settings > Control > Quarantine**.
2. Mark the **Enable Quarantine VLAN Switching** check box with a check mark to enable it.

3. If you need to set all hosts to safe, click **Apply**.
4. Click **Save Settings**.

Settings

Option	Definition
Quarantine VLAN Switching	When quarantine VLAN Switching is set to Enable and the ports are in the Forced Remediation Group, the appliance switches unregistered hosts that are being scanned to the quarantine VLAN until the scan process is completed. Registered hosts are scanned in the production VLAN. Once the scan is finished and the registered host has passed, the host remains in the production VLAN. If the host fails the scan, it is moved to the quarantine VLAN to remediate. When set to Disable, all hosts remain in the production VLAN during the scan process even if the host fails the scan. Default =Enable
Set all hosts 'Risk State' to 'Safe'	'Risk State' to 'Safe' Changes all hosts to Safe. Note: The status of the individual scans for each host remain unchanged.

Network device

Network Device allows you to set global properties that are specific to network devices and VLANs.

1. Click **Network > Settings > Network Device**.
2. Click a field and enter a setting. See the table below for settings.
3. Click **Save Settings**.

Settings

Field	Definition
Agent Switching Delay (Sec)	Number of seconds FortiNAC waits before a host that has failed the Persistent Agent Check will be switched to the Quarantine or Remediation VLAN. Default = 0 seconds
Minimum Trap Period (Sec)	Number of seconds FortiNAC waits after receiving a linkup trap before reading the forwarding table from the switch associated with the trap. Default setting = 10 seconds
Max Number of Trap Periods	Maximum number of Trap Periods that the appliance waits before reading the switch forwarding tables. If the switch does not have the MAC address information for the port that generated the linkup trap, the appliance places the switch back into the queue. Once the Minimum Trap Period has expired, the forwarding table on the switch is read again. If another linkup trap is generated by the same switch the trap period time is reset. Default setting = 4 For example, if the Minimum Trap Period is set to 20 seconds and the Max Number of Trap Periods is set to 2, the longest the appliance will wait to read the switch forwarding tables is 40 seconds.
Cold Start/Warm Start Trap Delay (Sec)	After receiving a Cold/Warm Start trap, FortiNAC waits for the amount of time specified in that field before polling the switches. Note: When the L2 poll is scheduled at the same time the delay is in progress, the poll gets delayed until the Cold Start/Warm Start Trap Delay interval is finished.
Registration Delay (Sec)	Number of seconds FortiNAC waits before switching a port to the production VLAN. This allows the user registering a host time to read the information on the Registration Success page. Default setting = 5 seconds If another host connects to the same switch during the Registration Delay time, the switch updates and the port is switched to the production VLAN without waiting for the delay time to expire.
System Defined Uplink Count	When the number of MAC addresses on a port exceeds this value the port is changed to an uplink. Setting this value to a higher number can help to indicate Multi-Access points. Default setting = 20

Field	Definition
	For example, setting this value to 7 changes the port to an uplink if a minihub with 8 ports is connected on the port. See Port properties on page 360.
Telnet Connection Timeout (Sec)	When using telnet to contact devices, this setting determines how long the server waits for a response from the device before timing out. Default = 12 seconds
VLAN Reset Delay (Sec)	Number of seconds FortiNAC waits before resetting the VLAN of a port that has no connected hosts or devices. The port must be a member of either the Reset to Registration group or the Reset to Default port group. If the port is a member of both groups, the Registration VLAN takes precedence. Default = 60 seconds
VLAN Switching Delay (Sec)	Number of seconds FortiNAC waits between disabling and reenabling a port when switching it to another VLAN. Default setting = 8 seconds If this value is left as zero (0) the host may have an invalid IP on the new VLAN.
MAC address Spoof Time Delay (Minutes)	Supported for wired connections only. The default is set to 5 minutes. Non-zero value: The number of minutes after which, if the same MAC address has been detected on two devices/ports simultaneously on two different switches, the Possible MAC address Spoof event will be generated. Workflow: - Two devices connect with the same MAC address: one to switch A and on to switch B - L2 poll of switch A (detects one of the devices) - L2 poll of switch B (detects the other device) - Wait the number of minutes specified by MAC address Spoof Time Delay value - L2 poll of switch A - L2 poll of switch B - If the MAC address is still detected in both locations, Possible MAC address Spoof event is generated Note: - An event will not be generated if both devices with the same MAC address are connected to the same physical switch. - A long age time in a host may cause the MAC address of the host to be falsely reported as connected to more than one device at the same time. For example, Host A is connected to Switch A with an age time of 10 minutes. Host A is moved to Switch B and FortiNAC updates the location. FortiNAC reads Switch A which still shows Host A as online because Host A has not yet aged out. Zero (0) value: (Recommended - available in FortiNAC Versions 8.8.8, 9.1.2 and above) Enables two features: - The Possible MAC address Spoof event will be generated on every connection move that occurs on an L2 Poll. - The Possible MAC address Spoof event will be generate on a connection move, that occurs on the same physical Switch.

Field	Definition
Enable Multi-Access Detection	When enabled, the appliance looks for multiple MAC addresses on ports each time a switch is read. Default = Disabled To have an event generated when multiple MAC addresses are detected on a port the Multi-Access Point Detected event must also be enabled. However, if the port is in the Authorized Access Points group an event is not generated. See Event management on page 772 to enable the Multi-Access Point Detected event. See System groups on page 851 to determine if the port is in the Authorized Access Points group.
Multi-Access Detection Threshold	The number of MAC addresses that are allowed on a port before a Multi-Access Point Detected event is generated.
Enable Cisco Discovery Protocol	When enabled, allows FortiNAC to query devices about other connected devices on the network. If a device has this discovery protocol enabled it gathers and stores information about devices it manages and devices it can contact on the network. Only devices with CDP enabled will respond to a CDP query. This is a global setting for the system. If this setting is enabled, devices can be set individually on the Polling Tab of the Device Properties View. If this setting is disabled, the device setting is ignored and the CDP feature is not used when polling a device. Devices that have the capacity for CDP must have the feature configured on the device's firmware. Default = Enabled
Enable Link Layer Discovery Polling	When enabled, allows devices to advertise information and their identity to neighboring devices connected to the same network.
Maximum Cisco Discovery Depth	Limits the number of layers from the original device that will be queried using Cisco Discovery Protocol. For example, if the Depth is set to 1, then FortiNAC will only query for devices that are directly connected to the device with the starting IP address during the Discovery process. If the Depth is set to 2, then FortiNAC stops querying after it reaches the second level of devices away from the starting IP address. See Discovery on page 311.
Ignore MAC Notification Traps for IP Phones	When enabled, FortiNAC will not process MAC Notification Traps for IP Phones. This setting is enabled by default. Disabling this setting may cause FortiNAC to process large numbers of traps, resulting in decreased performance.
Enable Network Access Policy for Wireless Access Points	When enabled Network Access Policies will be applied to Wireless Access Points connected to the network. Note the port it is connected to must be a member of the Role-Based Access group.
Wireless Access Point Enforcement Group	A port group which will be populated when a Wireless Access Point is connected. The port it connects to will be added to the group. The port will not be automatically removed from the group.
Preserve Port Names	Enabled by default. When disabled, any port names/labels that have been changed on the switch will be updated in the FortiNAC database upon the next "Resync Interfaces". Affects all device models when modified in this view. To modify at the device model level, see Device properties.

Field	Definition
	Note: Does not apply to ports on FortiSwitch in either Standalone or FortiLink mode. This is due to a difference in how port names are handled in the FortiSwitch.

Persistent Agent

Persistent Agent groups together properties for the use and behavior of the Persistent Agent and the configuration for updating the Persistent Agent installed on existing hosts to a different version.

Navigate to **System > Settings > Persistent Agent**.

Options

Option	Definition
Agent Update	Globally update hosts on your network that already have a Persistent Agent installed. See Agent update on page 913 .
Credential Configuration	Configure how credentials are verified for hosts who use the Persistent Agent. See Credential configuration on page 918 .
Properties	Configure the following: • Host name of the server for Persistent Agent communication. • Host group whose members receive the host name when they connect. • Whether display notifications will be sent to the host. • Header and footer text for the Persistent Agent authentication page. • Status messages in the message box on the user's desktop. See Properties on page 919 .
Status Notifications	Use the Status Notifications view to configure how users are notified of their host status when the Persistent Agent contacts the FortiNAC server. See Status notifications on page 924 .
Transport Configuration	Configure TCP and UDP communication between the FortiNAC server and the Persistent Agent. See Transport configurations on page 926 .
USB Detection	Use the USB Detection view allows to configure FortiNAC to be notified in the event that a USB device was plugged into a host on the network. See USB detection on page 929 .

Agent update

Hosts on your network that already have a version of the Persistent Agent installed can be globally updated. The update is triggered when a host connects to the network and the current Persistent Agent begins to communicate with FortiNAC.

The Persistent Agent version number on the host is checked by FortiNAC. If the version is different than the one selected on the Agent Update window, an update is initiated.

Clients upgrading the Persistent Agent must have access to Port 80 on the FortiNAC appliances.

It is only the difference in version number that triggers the update. FortiNAC does not check to see if the existing number is higher or lower than the update. This allows you to go back to a previous Persistent Agent if necessary.

If the host has software installed to reset the host to its original configuration after a re-boot, the agent reverts to the previous version. The software must be disabled before updating the Agent.

Update failure

A maximum number of attempts to update limits the number of times FortiNAC tries to update the host. If the maximum number of attempts has already been met, then no update is sent.

To address this you have several options. If a large number of hosts have failed the update, use **Reset Counter** on the Agent Update window to set the counter for all hosts to 0. If only a few hosts have failed the update, the Agent Version can be updated individually. Another option is to increase the Maximum Attempts on the Agent Update window to force an update. However, if the original problem has not been addressed the update will probably fail again.

Reset hosts that failed to update

If you have a large number of hosts that failed to update successfully and the Maximum Global Update Attempts count for those hosts was exceeded, the counter can be reset allowing the system to try to update those hosts again. The counter is reset for all hosts in the database; however, the system will not attempt to update hosts that successfully updated earlier.

1. Click **System > Settings**.
2. Expand the **Persistent Agent** folder.
3. Select **Agent Update** from the tree.
4. Click **Reset Counter**.

Event generation

When an update fails because the maximum number of attempts has been met, an **Agent Update Failure** event is generated. The default setting for this event is Enabled. See [Enable and disable events on page 773](#) to modify the default setting. Enabled events are recorded and can be viewed. See [Events on page 749](#).

When an update is successful an **Agent Update Success** event is generated. The default setting for this event is Disabled. Disabled events are not recorded and cannot be viewed later.

Alarms can be associated with enabled events. See [Map events to alarms on page 784](#). Alarms can be configured to send e-mail notifications or simply display on the dashboard in the **Alarm** panel.

Set up global updates

1. Click **System > Settings**.
2. Expand the **Persistent Agent** folder.
3. Select **Agent Update** from the tree.
4. Click the check box(es) to enable an update.
5. Click in the drop-down box and select the Persistent Agent Version for the update.
6. Click in the **Maximum Global Update Attempts** field and enter the number of times the update feature should attempt to update the Persistent Agent for each host.
7. If you need to trigger the installation of an earlier version of the Agent, click **Allow Installation of a Previous**

Version and make sure the correct version is selected in the version fields. Typically this would remain unchecked because you would want to move to the newest version of the Agent.



If you have selected **Latest Persistent Agent** as the agent to download on the **Endpoint Compliance Configuration** window for any configuration, you should not check this option.

Your hosts could end up in a situation where the latest agent is installed based on the endpoint compliance policy used when the host is registered, then an older agent is installed because this option is checked and the agent selected is older than the latest agent.

8. Click **Save Settings**.

Settings

Field	Definition
Modify Global Agent Update Exceptions	Opens the Global Agent Update Exceptions Group and allows you to add or remove hosts. This group can also be modified from the Groups View. Hosts in this group are never automatically updated. See the Exclude Hosts From the Update section below this table.
Update Windows Agents To Version	If enabled, Windows hosts with a Persistent Agent installed will be updated if the version number on the agent currently installed is different than the version selected in the drop-down list. A lower agent version will not be installed unless the Allow Installation of a Previous Version option is checked.
Update macOS Agents To Version	If enabled, macOS hosts with a Persistent Agent installed will be updated if the version number on the agent currently installed is different than the version selected in the drop-down list. A lower agent version will not be installed unless the Allow Installation of a Previous Version option is checked.
Maximum Global Update Attempts	Number of times FortiNAC should attempt to update the Persistent Agent for each host. If the maximum is reached and some hosts have not been updated, use Reset Counter to clear the number of attempts for all hosts and try again.
Allow Installation Of A Previous Version	If enabled, FortiNAC will update the agent on a host even if the installed agent is a higher version than the agent selected for update.
Reset The Hosts Update Counter To 0	Clear the number of update attempts from the Host record for all hosts. This allows FortiNAC to attempt to update hosts that were not successfully updated previously. See the Reset Hosts That Failed To Update section above this table.
Schedule Auto-Definition Updates	Allows you to schedule updates that include: • Information on the latest antivirus definitions • Support for new versions of antivirus • Support for new operating system versions • Any new vendor OUIs released by the IEEE Standards Association • New or modified custom scan options

Exclude hosts from updates

A special group, **Global Agent Update Exceptions**, has been created to stop selected hosts from being automatically updated. Any host in this group is not updated. This is controlled by MAC address. If a host has more than one MAC address, as long as any one of its MAC addresses is listed in this group the host is not updated.

The user name of the person who logs into this host displays along with the MAC address in the Group window. However, the user name is actually ignored for update purposes. If a user logs into a second different host, the second host is updated because none of its MAC addresses match anything in the Global Agent Update Exceptions group.

1. Click **System > Settings**.
2. Expand the **Persistent Agent** folder.
3. Select **Agent Update** from the tree.
4. Click **Modify Global Agent Update Exceptions**.
5. In the Group dialog, select one or more hosts from the column on the left.
6. Click the right arrow in the center of the dialog to move them to the Selected Members column.
7. Click **OK** to save.

This group can also be modified from the Groups View.

Verify the number of updated hosts

Since hosts are only updated when they connect to the network, updating all hosts could take some time. To see how many hosts have been updated, go to the dashboard and look at the Persistent Agent Summary panel. This displays the total number of hosts registered and breaks that number up into groups by version number and operating system. If the panel is not displayed, use the Add Panel link to restore it to the dashboard.

Schedule auto-definition updates

This feature allows you to automatically update the Virus Definition or Signature information for the antivirus software that is permitted in Scans within your endpoint compliance policies.



When new versions of an operating system and antivirus are added using the Auto-Def Schedule feature, they are not automatically selected in existing scans. You must go to each scan and enable the new options if you choose to scan for them.

The scans you configure with endpoint compliance specify the definition requirements for antivirus programs as well as operating systems. The default setting for the definition version information for all supported antivirus products is updated when the scheduled Automatic Definition Synchronizer task runs.

This task applies the update to all configured scans. The version information is maintained by Fortinet and is updated on a weekly basis. It is recommended that this task be scheduled to run weekly. If you change the default information in a scan for a specific operating system or antivirus software, the scheduled task will not overwrite that change.

To have the most recent version information appear in the Scan, go to the Scan containing the modified operating system or antivirus program, deselect the program and click OK. Open the Scan again and reselect the program. Click OK again to restore all the default settings for the selected program.

Automatic updates rely on the configuration of communications settings between the FortiNAC server and the updates server. See [Agent updates on page 1001](#) for information on configuring communications.

Configure Schedule

1. Click **System > Settings**.
2. Expand the **Persistent Agent** folder.
3. Select **Agent Update** from the tree.
4. Click **Modify Schedule**.
5. Select the **Enabled** check box.
6. Enter a name for the task in the Name field.
7. The **Description** field is optional. Enter a description of the task.
8. Action type and Action are pre-configured based on the task and cannot be modified.
9. From the **Schedule Type** drop down list, select either **Fixed Day** or **Repetitive** and set the day and time that the task is to be performed.
10. A **Fixed Day Task** is one in which you schedule a task to run on a combination of days of the week and times of the day, such as Mondays at 1:00 pm and Fridays at 10:00 am. Select the day(s) and time to run the task.
 - a. Click the **box** next to the day(s) to select the day.
 - b. Click the **down arrows** and select the hour, minutes, and AM or PM from the drop-down list for each day.
 - c. To enter days/times more quickly, select **Set Multiple Days** to set multiple days with the same time.
 - d. To remove all settings, click **Clear All**.
11. A **Repetitive Task** is one that you schedule to start on a given day, at a certain time, for the number of times you specify, such as every 10 days starting today. The repetition rate can be set to any number of minutes, hours, or days.
 - a. Enter the **Repetition Rate** using whole numbers.



A repetition rate of zero causes the task to run only once.

- b. Click the **down arrow** and select **Minutes**, **Hours**, or **Days** from the drop-down list.
- c. Enter the **date and time** for the task to run in the **Next Scheduled Time** field using the format MM/DD/YY hh:mm AM/PM Time Zone.



The new Repetition Rate does not take effect immediately. It starts the next time the scheduled task runs. For the new Repetition Rate take effect immediately, click **Update**.

- d. Click **Update** to update the Next Scheduled Time field or change the Repetition Rate.
12. Click **OK**.

Schedule settings

Field	Definition
Remove local backups older than	Number of days for which you would like to keep backups. Anything older than the number of days entered, is removed the next time the scheduled task for backups runs. This setting removes backup files created on the FortiNAC server before they are copied to the remote server. Backups on the remote server are not removed. The timing of the scheduled backup task and the age of the files that are to be removed must be thought out carefully or you will remove all of your backups. For example, if the remove option is set to 5 days and your backup task runs every 15 days, you may inadvertently remove all of your backups. However, if the remove option is set to 15 days and the backup task runs every 5 days, then you would always have backup files.
Status	Indicates whether the task is enabled or disabled.
Schedule Interval	How often the scheduled task runs.
Next Scheduled Time	The next date and time the scheduled synchronization task will run. Entered in the format MM/DD/YY HH:MM AM/PM
Modify Schedule	Allows you to modify the scheduled activity.
Run Now	Runs the scheduled task immediately.

Credential configuration

Configure how credentials are verified for hosts who use the Persistent Agent.

1. Click **System > Settings**.
2. Do one of the following:
 - a. In folder view, expand **Persistent Agent** and select **Credential Configuration** from the tree.
 - b. In flat view, select **Credential Configuration - Persistent Agent**.
3. Use the table below to configure Persistent Agent Credentials and click **Save Settings**.

Settings

Field	Definition
Enable Registration	If checked, any unregistered (rogue) hosts who use the Persistent Agent will be registered by the agent. Typically this is disabled when rogues are being registered by the device profiler. There is a method in device profiler that detects the presence of the Persistent Agent and can use that in combination with other criteria to register the host. When this option is unchecked, Register as Device and Authentication Type are disabled.
Register As Device	If checked, all unregistered (rogue) hosts who use the Persistent Agent are registered automatically when they connect to the network. Then name of the host is entered in the ID field in the host record.

Field	Definition
	If unchecked, all unregistered (rogue) hosts who use the Persistent Agent are presented with a login screen to enter their credentials. The credentials are verified with the method selected in the Authentication Type field.
Authentication Type	The method used to verify the user credentials for access to the network. Method must match the "Standard User Login Type" method selected under Portal > Portal Configuration > Global > Settings. See Configure authentication credentials. Available Options: Local - Validates the user to a database on the local FortiNAC. Use this option if you plan to enter a list of registered users. LDAP - Validates the user to a directory database. FortiNAC uses the LDAP protocol to communicate to an organization's directory. RADIUS - Validates the user to a third party RADIUS server. For defining 3rd party RADIUS server profiles, see Proxy. This option is not available for Local RADIUS. RADIUS/LDAP - Indicates that the user is being authenticated by a third party RADIUS server but registered based on data in an LDAP server. If the user is successfully authenticated by the RADIUS server but does not exist in the LDAP database, FortiNAC will still create the user record in its own database. Google authentication for the Persistent Agent is not supported.

Properties

Use properties to set:

- The host name of the server for Persistent Agent communication.
- The Host group whose members receive the host name when they connect.
- Whether to require an adapter to be connected to a device managed by FortiNAC in order to communicate.
- Whether display notifications will be sent to the host.
- Header and footer text for the Persistent Agent authentication page.
- The amount of time that a CRL will be cached before retrieving a new CRL.
- Status messages in the message box on the user's desktop.

You can also enter text for other message windows generated during Registration or Scanning.

To access Persistent Agent properties, go to **System > Settings > Persistent Agent**.

Settings

Field	Definition
Primary Host Name	Fully qualified host name of the FortiNAC Application Server or the FortiNAC Server if you are not using a pair. It is pushed out to the connecting host(s) to ensure that the Persistent Agent is communicating with the correct host in a distributed environment. In a high availability environment you must use the actual host name not the shared host name. This field is required for Agent Updates.

Field	Definition
Secondary Host Name	This field is displayed only in a high availability environment and is used only in a failover situation. Fully qualified host name of the secondary FortiNAC Application Server or the secondary FortiNAC Server if you are not using a pair. It is pushed out to the connecting host(s) to ensure that the Persistent Agent is communicating with the correct host in a distributed environment. Use the actual host name and not the shared host name. This field is required for Agent Updates.
Host Group for on-connect Host Name update	When hosts in this group connect to the network, they are given this Persistent Agent host name for communication between the host and the Persistent Agent server.
Require Connected Adapter	If enabled, the server will require one of the adapters reported by the agent to be connected to a device managed by FortiNAC in order to communicate. This eliminates the need to use ACLs to block access to a FortiNAC Application server when the host is connecting on a device managed by a different FortiNAC Control server/Application server pair. The agent must be configured with security enabled. Requires Persistent Agent 4.0.3 or higher.
Allowed IP Subnets	When you have a client that is not detected as connected (e.g., a VPN-connected client), the agents cannot connect to the server when the Require Connected Adapter option is enabled. You can configure specific subnets to allow the server to accept connections from any host connecting from an IP address within one of the subnets or from any connected adapter. Any IP address that the agent connects from will be checked against these subnets. If the IP address is within the range, it will be allowed to connect. This applies to all hosts connecting from the specified ranges.
Expiration	If enabled, the Persistent Agent uninstalls itself from the host once date and time selected have passed. Note: Expiration is only supported for Windows and macOS.
Header	This text appears at the top of all message windows generated by the Persistent Agent.
Login Prompt	This text displays on the login window.
Login Prompt after Authentication Failure	This text appears in the message block received when a user has not been authenticated.
User Name Label	Controls the text that appears next to the User Name field on the log in window.
Password Label	Controls the text that appears next to the Password field on the log in window.
Footer	This text appears at the bottom of all message windows generated by the Persistent Agent.
CRL Cache Strategy	Defines the amount of time that a CRL will be cached before retrieving a new CRL. • Expire After Next Update. This is the default setting. Retrieves a new copy of the CRL when the date defined by the CA in the CRL has expired. • Expire After This Update. Select this option to define how long after the date defined

Field	Definition
	as This Update in the CRL when a new CRL should be retrieved. If the number of hours entered is fewer than the This Update time interval defined in the CRL, the CRL will be retrieved each time a scan occurs because the CRL will appear out of date. This may cause performance issues. • Poll for Changes. Sets the time interval to download a new CRL. • Update Cache. Lets you instantly retrieve a new CRL. This can be used when a certificate is revoked and you require a new CRL. Otherwise, the CRL is retrieved based on the defined Cache Strategy settings. See Certificate validation on page 504.
Agent Contact Window on Connect	Applies to host records identified as having the Persistent Agent installed. Default value: 600 seconds Time the agent on the endpoint device has to establish a connection with FortiNAC. This window of time starts when the endpoint device's host record status changes from offline to online. When the allotted window of time has passed without communication: • Host record's agent status is set to "No Contact" • "Persistent Agent Not Communicating" event is generated When agent starts communicating again: • Host record's "No Contact" agent status is cleared • "Persistent Agent Communication Resumed" event is generated Successful Connection   Unsuccessful Connection  
Agent Contact Window on Disconnect	Applies to host records identified as having the Persistent Agent installed. Default value: 300 seconds Time the agent on the online endpoint device has to communicate with FortiNAC. This window of time starts once FortiNAC detects the TCP session with the agent has been broken. When the allotted window of time has passed without communication: • Host record's agent status is set to "No Contact" • "Persistent Agent Not Communicating" event is generated When agent starts communicating again: • Host record's "No Contact" agent status is cleared • "Persistent Agent Communication Resumed" event is generated Successful Connection

Field	Definition
	 Unsuccessful Connection 
Agent Contact Window on Host Disconnect	Applies to host records identified as having the Persistent Agent installed. Default value: 30 seconds Time before clearing the "No Contact" agent status on an affected endpoint device's host record after disconnecting from the network. This window of time starts when the endpoint device's host record status changes from online to offline. When the allotted window of time has passed: Host record's "No Contact" agent status is cleared Unsuccessful Connection  Host disconnects from network (offline)  "No Contact" agent status is cleared 
VM Detection	None. When selected, a virtual machine that connects to the network as a bridged adapter is detected as a new device on the port. Append to Host. When selected, the virtual machine adapters are added to the host as additional adapters. When a Guest VM has been appended to the host as a virtual Guest adapter, the Guest VM will remain an adapter on that host until the Guest VM is manually deleted from the host, even if VM Detection is changed to None or Register as New Host. Register as New Host. When selected, the virtual machine is automatically registered as a new host belonging to the same user as the host running the virtual machine, allowing default registration. VM Platform Support by OS

Field	Definition																
	<table><tr><th>Platform</th><th>Windows</th><th>OSX</th><th>Linux</th></tr><tr><td>Oracle VBox</td><td>Supported</td><td>Supported</td><td>Supported</td></tr><tr><td>VMware Workstation*</td><td>Supported</td><td>Not Supported</td><td>Supported</td></tr><tr><td>VMware Fusion</td><td>Not Supported</td><td>Supported</td><td>Not Supported</td></tr></table> *VIX 1.5 must also be installed for Workstation Player VMware requirements: - Virtual machine must be configured with a bridged network adapter. - VMware VIX must be installed. *VIX 1.5 must be installed for Workstation Player - In %ProgramFilesx86%\VMWare\VMware VIX\vixwrapper-config.txt, set the 4th column (16.1.2 in the example below) to whichever version of workstation or player is installed. Example: <pre>ws 19 vmdb 16.1.2 Workstation-12.0.0 player 19 vmdb 16.1.2 Workstation-12.0.0</pre> Oracle VBox requirements - Oracle VM Virtualbox must be installed. Linux hosts must be configured to run the Persistent Agent Daemon process as the logged on user. To configure this, go to /etc/sysconfig/bndaemon and change DAEMON_USER from bndaemon to the current logged on user, and then restart the daemon service. FortiNAC will register a detected VM guest with the same registration as the VM host. However, the VM guest will not inherit the authentication state of the VM host, and the guest OS will be subject to any authentication policies currently in place. This means that the guest OS may require separate authentication.	Platform	Windows	OSX	Linux	Oracle VBox	Supported	Supported	Supported	VMware Workstation*	Supported	Not Supported	Supported	VMware Fusion	Not Supported	Supported	Not Supported
Platform	Windows	OSX	Linux														
Oracle VBox	Supported	Supported	Supported														
VMware Workstation*	Supported	Not Supported	Supported														
VMware Fusion	Not Supported	Supported	Not Supported														
Display Notifications	Determines whether the popup notifications from the Persistent Agent such as "VLAN switch taking place", or "Renewing IP", will be displayed. When checked the notifications are displayed on the host. If unchecked, the notification fields below are hidden on this configuration view and on the host.																
Successful Registration	This text appears in the message block received when a host has successfully registered. If you do not enter text, the message box does not appear for successful registrations.																
Failed Registration	This text appears in the message block received when a host has failed the registration process. If you do not enter text, the message box does not appear for failed registrations.																
Failed Scan	This text appears in the message block received when a host has failed a scan. If you do not enter text, the message box does not appear for failed scans.																
Warning Message	This text appears in the message block received when a host has warning messages generated from a scan. If you do not enter text, the message box does not appear for warning messages.																

Field	Definition
Remediation	This text appears in the message block received when a host has been placed in the Remediation VLAN. If you do not enter any text, the message box does not appear.
No Valid Network Interfaces found	This text appears in the message block when the Persistent Agent cannot determine the MAC address of the interface used to connect to the network or if the MAC address for that interface is invalid. Default value for this field is blank. If you do not enter text, the message box does not appear for invalid MAC addresses.
Network Change Message	This text appears in the message block when the IP address for the host is being renewed. This can happen when the host is being moved from one VLAN to another.
Enable VLAN Switch User Acknowledgment	(Persistent Agent versions 9.4.4, 10.7.2, F 7.6.0 & F 7.6.1) When selected, user is presented with a message that the network access is going to be switched. The message appears any time the VLAN switches. User is prompted to click "OK" to proceed. If user does not click either, the VLAN will switch after the number of seconds defined in the "Acknowledgement timeout" field. (FortiNAC version F 7.6.5 + & Persistent Agent version F 7.6.2 +) Determines whether the Persistent Agent will popup a user acknowledgment when VLAN is transitioning from a remediation VLAN. If enabled, an Event-to-Alarm Mapping can be enabled to prevent the VLAN change if the user cancels the acknowledgment or if the acknowledgment times out.

Configure properties

1. Click **System > Settings**.
2. Expand the **Persistent Agent** folder.
3. Select **properties** from the tree.
4. Use the information in the properties Settings table above to complete the fields.
5. Click **Save Settings**.

Status notifications

Use the status notifications view to configure how users are notified of their host status when the Persistent Agent contacts the FortiNAC server. There are two levels of notification. The first enables or disables the display of a special icon shown in the system tray based on the state of the host. If the first level is enabled, the second level enables or disables the display of Notification Balloons over the icon. These provide more detail to the user if there is an issue with network access.

Settings

Icon/Field	Definition
	This icon displays in the host system tray if special icon options have been enabled on the Status Notifications window. This icon represents the following host states: • Disabled • At Risk • Pending At Risk • Needs to Authenticate Icon can only be disabled using administrative templates.
	This icon displays in the host system tray. Indicates that the host has normal network access. If you require authentication, this icon also indicates that the user has been authenticated. Icon can only be disabled using administrative templates.
	This icon displays in the host system tray. Indicates that the host has been disconnected from the network. Icon can only be disabled using administrative templates. This icon will display for Agent 3.5 and higher.
Display a special "Disabled" icon when a host is disabled.	Displays an icon in the system tray indicating that the host has been disabled and does not have access to the network. The user must double-click on the icon or click on the notification balloon to open a web-browser with additional information.
Display a special "At Risk" icon when a host is at risk.	Displays an icon in the system tray indicating that the host has been marked At Risk based on an endpoint compliance policy scan. The user can double-click on the icon or click on the notification balloon to open a web-browser with additional information. For Persistent Agent with EasyConnect, it is recommended that you enable this check box to display a notification balloon that allows the user to access the web page to register upon failure to connect.
Display a special "Needs to Authenticate" icon when a host needs to authenticate.	Displays an icon in the system tray indicating that the user on this host has not been authenticated. The user can double-click on the icon or click on the notification balloon to open a login window.
Display a normal icon when host returns to normal.	Displays an icon in the system tray indicating that the host has normal network access and there are no issues.
Provide a Log Off functionality from the tray icon for authenticated hosts.	Allows authenticated users to log off the network by right-clicking the Persistent Agent icon and selecting Log Off the Network from the pop-up menu. This does not log the user out of Windows.
Display a special "Pending At Risk" icon when a host is pending at risk.	Displays an icon in the system tray indicating that the host has been marked Pending At Risk based on an endpoint compliance policy scan that has delayed remediation enabled.

Icon/Field	Definition
	The user can double-click on the icon or click on the notification balloon to open a web-browser with additional information. See Delayed remediation on page 546.
Display a special "Disconnected" icon when a host is disconnected.	Displays an icon in the system tray indicating that the host has been disconnected from the network. Requires Agent 3.5 or higher.
Display a Notification Balloon with content.	This option is provided for each icon and is available only when the Display Icon option above it has been enabled. If Notification Balloons are enabled enter the text you would like the user to see in a balloon when his host status changes. Balloons follow the Windows standards as far as the amount time they are displayed and disappearing when they are clicked. When a balloon is clicked it takes the user to either a web-browser with additional information or a login window.
Include logical network name in balloon notification (Requires agent version 9.4.4 or 10.7.2 or greater)	Displays the currently assigned logical network name in the balloon messages. This option is provided for each icon and is available only when the Display Icon option above it has been enabled. Balloons follow the Windows standards as far as the amount time they are displayed and disappearing when they are clicked. When a balloon is clicked it takes the user to either a web-browser with additional information or a login window.

Transport configurations

Packet Transport Configurations define the methods of communication available between FortiNAC and the Persistent Agent. Each Packet Transport Configuration is defined with a unique Name and a unique combination of Bind Address, Port, and Transport Type. If no Bind Address is specified, all addresses are bound for the supplied Port. The supplied port must be in the range of 1024 to 49151 and not already in use by another service within the operating system. If the Transport Type is TCP, a TLS Service Configuration must be defined to secure the communication. Changes made to Packet Transport Configurations do not take effect immediately. The enabled configurations will begin listening when the Persistent Agent services are reloaded or FortiNAC is restarted.

TLS Service Configurations define the certificate, TLS Protocols, and Ciphers used for secure communication. The certificate can be uploaded using the certificate Management view. By checking "Automatically Update Ciphers and Protocols on Upgrade," the settings for both Ciphers and TLS Protocols will become managed by FortiNAC. Upon upgrade, the system will automatically configure the TLS Service Configuration to the latest recommended Ciphers and Protocols.

TLS Service configurations apply to the following:

- PA Protocol Transport configurations
- Admin GUI (named with UUID)
 - Example: Admin UI f2xxx5-a986-4c6c-b2ea-xxxxxxx33b
- RADIUS Server configurations

Packet transport settings

Field	Definition
Enabled	If true, a listener will be created for this configuration on the next load of the Persistent Agent services.
Name	Unique name used to identify the configuration.
Bind Address	An optional IPv4 or IPv6 to use when listening for packets. If no address is provided, all addresses are used.
Port	The port this configuration should open a socket using. System and Dynamic ports may not be used. Valid values are in the range of 1024 to 49151.
TLS Configuration	The selected configuration for security communication with the Persistent Agent. Only TCP transports use a TLS configuration.
Maximum Incoming Packets to Queue	The maximum number of unprocessed packets from the Persistent Agent to retain. Any packets received while the queue is full will be discarded.
Read Idle Timeout	The maximum amount of time, in seconds, without receiving from the agent before closing the connection.
Write Idle Timeout	The maximum amount of time, in seconds, before the server will send a packet to the agent to ensure the connection is still open.
Use Native Transport (Experimental)	Use native libraries for Sockets and TLS when possible. Enable this experimental feature only if recommended.
Last Modified By	User name of the last user to modify the configuration.
Last Modified Date	Date and time of the last modification to this configuration.

Right click options

Modify	Modify the selected Packet Transport Configuration.
Delete	Deletes the selected Packet Transport Configuration.
Reload Services	Closes any existing sockets in the Persistent Agent server and creates a new series of sockets using the enabled Packet Transport Configurations. All unprocessed packets in the existing queues are dropped, allowing the Persistent Agent server to resume communication from a clean state.
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746 .



You must have permission to view the admin auditing log. See [Add an administrator profile on page 139](#).

TLS service settings

Field	Definition
Automatically Update Ciphers and Protocols on Upgrade	If true, the settings for both Ciphers and TLS Protocols will become managed by FortiNAC. Upon upgrade, the system will automatically configure the TLS Service Configuration to the latest recommended Ciphers and Protocols.
Name	Unique name used to identify the configuration.
Ciphers	The Cipher Suite to use when encoding messages using TLS. At least one Cipher must be selected. Ciphers must be supported by both client and server, so disabling Ciphers may prevent some Persistent Agents from communicating.
TLS Protocol	The list of TLS Protocols to allow by the server. At least one TLS Protocol must be selected. TLS Protocols must be supported by both client and server, so disabling Protocols may prevent some Persistent Agents from communicating.
Certificate Alias	Select the certificate to use when securing communication. Note: It is possible to apply the certificate using the Portal alias to the TLS Configuration. However, selecting the Portal certificate alias does not apply the TLS configuration to the Portal itself. Certificates may be uploaded using the certificate management view. See Certificate management on page 828 .
Last Modified By	User name of the last user to modify the group.
Last Modified Date	Date and time of the last modification to this group.

Right click options

Modify	Modify the selected TLS Service Configuration.
Delete	Deletes the selected TLS Service Configuration.
In Use	Provides a list of Packet Transport Configurations that currently reference the selected TLS Service Configuration.
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746 .



You must have permission to view the admin auditing log. See [Add an administrator profile on page 139](#).

Add or modify packet transport configuration

1. Click **System > Settings**.
2. Expand the **Persistent Agent** folder.
3. Select **Transport Configuration** from the tree.
4. **To modify a record:** Select a Packet Transport Configuration record from the table and click **Modify**.
5. **To add a new record:** Click **Add** at the bottom of the upper panel.

6. Use the Settings for the Persistent Agent Transport Configuration topic to enter the Packet Transport Configuration information.
7. Click **OK** to save.

After adding or modifying a Packet Transport Configuration, the services will continue to use the previous configuration until a reload is requested or FortiNAC is restarted.

Delete packet transport configuration

1. Click **System > Settings**.
2. Expand the **Persistent Agent** folder.
3. Select **Transport Configuration** from the tree.
4. Select a Packet Transport Configuration record from the table
5. Click **Delete** at the bottom of the panel.
6. Click **Yes** on the confirmation message.

Add or modify TLS service configuration

1. Click **System > Settings**.
2. Expand the **Persistent Agent** folder.
3. Select **Transport Configuration** from the tree.
4. **To modify a record:** Select a TLS Service Configuration record from the table and click **Modify**.
5. **To add a new record:** Click **Add** at the bottom of the lower panel.
6. Use the Settings for the Persistent Agent Transport Configuration topic to enter the TLS Service Configuration information.
7. Click **OK** to save.

After adding or modifying a TLS Service Configuration, the Packet Transport Configuration services will continue to use the previous configuration until a reload is requested or FortiNAC is restarted.

Delete TLS service configuration

1. Click **System > Settings**.
2. Expand the **Persistent Agent** folder.
3. Select **Transport Configuration** from the tree.
4. Select a TLS Service Configuration record from the table
5. Click **Delete** at the bottom of the panel.
6. If one or more Packet Transport Configurations are associated with the TLS Service Configuration, you will not be able to delete it.
7. Click **Yes** on the confirmation message.

USB detection

The USB Detection view allows you to configure FortiNAC to be notified in the event that a USB device was plugged into a host on the network. When a USB drive is detected, FortiNAC events can be mapped to alarms to specify an action based on the host where the USB drive is connected. You can also indicate which drives should be ignored by the system, regardless of the hosts they are connected to.

This feature requires Agent 3.3 or higher. This feature is only supported on Windows hosts.

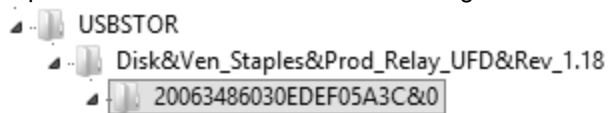
Settings

Icon/field	Definition
Enable USB Detection	When enabled, if a USB drive is plugged into a host, the agent will detect the USB drive and notify FortiNAC.
Prevent Detection on Host Group	Select the host group where you wish to prevent USB detection. If the USB connects to a host within the selected host group, the USB is ignored and no event is generated. Click the Add icon to add a group. Click the Modify icon to modify the selected group.
Event to alarm mappings	
USB Drive Detected	Allows user to configure an event to alarm mapping for when the USB drive is present when the agent is started.
USB Drive Added	Allows user to configure an event to alarm mapping for when the USB drive is added while the agent is running.
USB Drive Removed	Allows user to configure an event to alarm mapping for when the USB drive is removed while the agent is running.
Allow USB drives	
Name	Policy name for allowed USB drives.
Device ID	The Device ID for the USB drive from the registry key.
Device Class	The Device Class for the USB drive from the registry key.
Friendly Name	The Friendly Name for the USB drive from the registry key.
Right click options	
Delete	Deletes the selected USB drive.
Modify	Opens the Modify Allowed USB Drive dialog.
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746 .
 You must have permission to view the admin auditing log. See Add an administrator profile on page 139.	
Buttons	
Save Settings	Click to save the USB detection settings.

Add/modify an allowed USB drive

1. Click **System > Settings**.
2. Expand the **Persistent Agent** folder.

3. Select **USB Detection** from the tree.
4. Click **Add** or select an existing USB drive and click **Modify**.
5. Enter the name for FortiNAC to use to identify the USB drive that is being allowed.
6. Run `regedit.exe` to access the registry key.
7. Expand `HKEY_LOCAL_MACHINE>SYSTEM>CurrentControlSet>Enum>USBSTOR`
If `CurrentControlSet` is not available, you can also find `USBSTOR` in `ControlSet001`.
8. Expand the folder for the device containing the information you wish to add or modify, and click the key.



The key values appear.

Name	Type	Data
(Default)	REG_SZ	(value not set)
Capabilities	REG_DWORD	0x00000010 (16)
ClassGUID	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}
CompatibleIds	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW GenDisk
ConfigFlags	REG_DWORD	0x00000000 (0)
ContainerID	REG_SZ	{87d86d3f-e78a-5113-99fd-57126daaaafd}
DeviceDesc	REG_SZ	@disk.inf,%disk_devdesc%;Disk drive
Driver	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}\0001
FriendlyName	REG_SZ	Staples Relay UFD USB Device
HardwareID	REG_MULTI_SZ	USBSTOR\DiskStaples_Relay_UFD____1.18 USBST...
Mfg	REG_SZ	@disk.inf,%genmanufacturer%;(Standard disk driv...
Service	REG_SZ	disk

The asterisk (*) wildcard can be used at the beginning and end of all values you enter.

9. Enter the following values from the registry key:
 - Device ID: The first value from the Hardware ID key as defined in the Registry entry for the USB device in: `HKEY_LOCAL_MACHINE>SYSTEM>CurrentControlSet>Enum>USBSTOR` (e.g., `USBSTOR\DiskStaples_Relay_UFD____1.18`).
 - Device Class: The value from the Class key as defined in the Registry entry for the USB device in `HKEY_LOCAL_MACHINE>SYSTEM>CurrentControlSet>Enum>USBSTOR`
If the class value is empty or is not present in the registry, leave the Class field blank. Otherwise, the rule will not match and an event will be generated.
 - Friendly Name: The value from the friendly name key as defined in the registry entry for the USB device in `HKEY_LOCAL_MACHINE>SYSTEM>CurrentControlSet>Enum>USBSTOR`
10. Click **OK**.

Import allowed USB drives

You can import multiple USB drives at a time to the list of Allowed USB drives.

1. Click **System > Settings**.
2. Expand the **Persistent Agent** folder.
3. Select **USB Detection** from the tree.
4. Click **Import**.
5. Enter the Name, Device ID, Device Class, and Friendly Name for each USB drive you wish to import in the specified

format.

6. Click **OK**.

Delete an allowed USB drive

1. Select **System > Settings**.
2. Expand the **Persistent Agent** folder.
3. Select **USB Detection** from the tree.
4. Select a USB drive in the Allowed USB Drives list, and click **Delete**.
5. A confirmation message is displayed. Click **Yes** to continue.

Reports

Reports groups together properties for reports that are generated directly from the FortiNAC database.

Note: As of December 5, 2019, Fortinet discontinued the sale of the FNAC Analytics Reporting solution and recommends FortiAnalyzer as the FortiNAC reporting platform. For details, refer to the Product Life Cycle document found in the Fortinet Support Portal at: <http://support.fortinet.com/>

Option	Definition
Analytics	Configures the connection between the FortiNAC server and the Analytics server. This connection allows an agent on the FortiNAC server to push data for reporting to an external server based on a user-defined schedule.

Analytics

Use analytics to configure the connection between the FortiNAC server and the cloud reporting Analytics server. This connection allows an agent on the FortiNAC server to push data for reporting to an external server based on a user-defined schedule. The schedule is set in the Analytics reporting software.

1. Click **System > Settings**.
2. Expand the **Reports** folder.
3. Select **Analytics** from the tree.
4. Use the Settings table below to enter the connection settings for the Analytics server.
5. Click **Save Settings**.

Settings

Settings

Field	Definition
Activation Key	Key that activates the license for Analytics. When the license is activated, the agent on the FortiNAC server can begin sending data to the FortiNAC Analytics database. See Generate An Activation Key below for instructions on creating a

Field	Definition
	key.
Server	FQDN of the server where your FortiNAC Analytics database resides. Default = analytics.example.com.

Generate an activation key

1. On the FortiNAC Analytics server, log into the User Interface as Administrator.
2. Click the **Manage > Manage Client** on the menu bar.
3. Select the appropriate client from the list and click **Edit**.
4. On the Manage Clients view, click **Generate** under **Access Key**.
5. A license key is generated and displayed.
6. Highlight the text and copy it to the Activation Key field in FortiNAC under **System > Settings > Reports > Analytics**.
7. Click **Save Settings**.

System communication

System Communication groups together features that allow FortiNAC to communicate with other devices or to send email and SMS messages to administrators and network users.

Receive data from external devices

FortiNAC can be configured to receive data or messages from other devices on the network, such as an IPS/IDS device. FortiNAC can accept data from a trap or Syslog message to add records to the database or trigger events and alarms. If events and alarms are triggered, alarms can be configured to take action on hosts or users and notify administrators via e-mail or SMS messages.

There are several options that can be used to leverage data from other devices. Each of these options is independent of all of the others. They can be used simultaneously but they do not work together.

Syslog management

The Syslog Management feature in FortiNAC allows you to create specific configurations used to parse inbound syslog messages. Supported message formats include CSV, TAG/VALUE and CEF. New events and alarms are automatically created for each syslog configuration you create. When an inbound message is received, FortiNAC can react based on the event and alarm generated. See [Syslog files on page 963](#).

Trap MIB

The Trap MIB feature allows you to configure FortiNAC to receive SNMPv1 and SNMPv2 traps from external devices that contain information about the connecting host. New events and alarms are created for these configurations and they display based on the OID of the sending device. When a trap is received FortiNAC can react based on the event and alarm generated. See [Trap MIB files on page 973](#).

SNMPv3

SNMPv3 traps can be leveraged to populate the FortiNAC database with hosts and users as they connect to the network. When a trap is received from an external device, host and user records are added, modified or removed in the database. Events and alarms associated with these traps can be used to notify administrators or take actions on connecting hosts and users.

MDM services

MDM Services allows you to configure communication with one or more Mobile Device Management servers. Based on the information received from the MDM server you can take action on hosts, such as disabling them. See [MDM Servers on page 413](#).

Option	Definition
Addresses	Configure a list of address and address group objects used in SSO and VPN configuration. See Addresses on page 935
Email Settings	Enter settings for your email server. This allows FortiNAC to send email to Administrators and network users. See Email settings on page 937 .
Log Receivers	Configure a list of servers that to receive event and alarm messages from FortiNAC. See Log receivers on page 938 .
MDM Services	Configure one or more Mobile Device Management (MDM) servers that integrate with FortiNAC. See MDM Servers on page 413 .
Mobile Providers	Displays the default set of Mobile Providers included in the database. FortiNAC uses the Mobile Providers list to send SMS messages to guests and administrators . The list can be modified as needed. See Mobile providers on page 1 .
Patch Management	The Patch Management feature allows integration with Patch servers such as BigFix or PatchLink. See Patch management on page 940 .
Proxy Settings	Configure FortiNAC to direct web traffic to a proxy server in order to download OS updates and auto-definition updates.
SSH Key Management	Centralized SSH Key management system that securely generate, store, and manage SSH Keys for FortiGate Integration Please see SSH Key Management on page 947 .
SNMP	Set the SNMP protocol for devices that query FortiNAC for information. It is also used to set the SNMP protocol to accept SNMPv3 traps that register hosts and users. See SNMP on page 948 .
Syslog Files	Syslog Files that you create and store are used by FortiNAC to parse the information received from these external devices and generate an event. The event can contain any or all of the fields contained in the syslog output and can be mapped to an Alarm and an Alarm action. See Syslog files on page 963 and Map events to alarms on page 784 .

Option	Definition
Security Event Parsers	Customize parsing of syslog messages for generating security events. See Security event parsers on page 970
Trap MIB Files	Enter configurations to interpret SNMP trap MIB information sent from a device and associate it with events and alarms in FortiNAC. See Trap MIB files on page 973 and Map events to alarms on page 784 .
Threat Analysis Engines	Configure Threat Analysis Engines to be used when applications are submitted via an agent to FortiNAC.
Security Fabric Connector	Provides the ability to register FortiNAC in the Security Fabric Tree. Once registered, FortiNAC is visible in the Security Fabric Topology view on FortiOS products. See Security Fabric Connection on page 420

Addresses

1. Click **System > Settings**.
2. Expand the **System Communication** folder.
3. Select **Addresses** from the tree.

Introduced in version 9.2, address objects and address group objects are used in the following firewall integrations:

- FortiGate (SSO or VPN)

These objects are used to determine which firewall should receive SSO messages for hosts connecting to the network. Group objects allow for control over the network ranges and scopes used to filter SSO messages to each firewall.

Address objects can be created by subnet or by IP Range, then combined into address groups. The address groups can then be used within the Model Configuration view of the applicable device to define the scope to be managed. Groups are selected within the model using the SSO Addresses and VPN Addresses drop-down menus. See [Model configuration](#).

Object Auto-Population

By default, the Addresses tables are empty. It is up to the administrator to define the IP address scopes desired for SSO functionality.

Address and group objects will only auto-populate if SSO was configured prior to upgrading to version 9.2 or greater. This is to ensure previous SSO functionality is maintained:

- Prior to version 9.2, FortiNAC created internal address lists for SSO functionality. The objects are created using the same rules upon upgrade.
- These rules include reading the FortiGate interface IP scopes and VPN configurations to determine what addresses need to be created.
- All changes to the objects after they are created must be made manually.
- Changes take effect during the next endpoint evaluation. This occurs after the L2 poll of the device to which the affected endpoints are connected.

Add or Modify Address Object

Configure using the table below then click OK.

Field	Description
Name	Name of Address object
Message Type	Subnet or IP Range
IP/Netmask	Displays when Message Type Subnet is selected. Enter desired subnet and mask. Required Format: <IP address>/xx (CIDR) Example: 10.25.24.1/24
IP Range	Displays when Message Type IP Range is selected. Enter IP range <Starting IP address> – <Ending IP address> Example: 10.25.24.1 – 10.25.24.30

Add or Modify Address Group

Configure using the table below then click **OK**.

Field	Description
Name	Name of Address Group
Members	Select the drill down menu for existing Address objects or select  to create a new address object. Multiple objects can be selected.

Identify the Address Group Using a Specific Address Object

Select the Address Object then select **In Use** above the **Address** table.

Example Result:

Address In Use

The Address 'FGT-IT:root:VLAN-BYOD' is in use by the following:

- Network Address Groups
 - SSOGRP:FGT-IT:root

Identify the Device Model or VDOM Using a Specific Address Group

Select the Address Object then select **In Use** above the **Address** table.

Sending Tags for Non-Local FortiGate Connections

By default, FortiNAC does not send tags to subnets that do not terminate at that FortiGate.

Example:

- Address group: 192.168.10.x
- Endpoint with IP address 192.168.10.85 connecting to a switch downstream of the FortiGate.
- Endpoint with IP address 192.168.10.90 connecting to a port on the FortiGate.
- Both endpoints send their traffic through the same FortiGate.

Result: FortiNAC will send a tag to the FortiGate for 192.168.10.90 but not 192.168.10.85.

To allow FortiNAC to send tags for endpoints not directly connected to the FortiGate, a CLI change is required. Use the global option tool to expand the scope.

1. Login to the CLI as admin.
2. Type


```
execute enter-shell
globaloptiontool -name sso.expand.scope -set true
exit
exit
```
3. In the FortiNAC UI, navigate to **Network > Inventory**.
4. Right-click on the FortiGate Device Model and select **Resync Interfaces**.

Certificate management

Field	Definition
Import OS CA Trust Store (checkbox)	Enabled by default. FortiNAC imports all the trusted CAs from the system's OS to its local keystore. This allows FortiNAC to trust well-known root CAs automatically. Once imported, the CA certificates are listed as Certificate Target "General Trusted CA" under System > Certificate Management > Trusted Certificates. Used for trusting SSL connections with modeled network devices. For additional details, see Trusted certificates.

Email settings

1. Click **System > Settings**.
2. Expand the **System Communication** folder.
3. Select **Email Settings** from the tree.
4. Use the table below to enter the necessary settings.
5. Click **Save Settings**.

Note: This feature can also be accessed in **Network > Service Connectors > Create New > Email Server**

Settings

Field	Definition
Email Server	Server used to send email notifications.

Field	Definition
Sender Email	Email address that appears as the sender in email sent from FortiNAC. You may want to configure an alias for this email address to better inform the recipient that the message is being sent from FortiNAC.
Authentication	If enabled, you must enter the user name and password for the email account used as the sender account.
User Name	User Name for the email account used as the sender account.
Password	Password for the email account used as the sender account.
Port	Port used for communication with the email server. This must match the port setting on the email server itself.
Connection Security	Used to encrypt email communication between the FortiNAC server and the email server. This setting must match the setting configured on your email server. Options are: None, SSL/TLS or STARTTLS.
Always Send as Sender Email	If turned off, contextual e-mail addresses will be used, such as sending as the sponsor of a guest.
Advanced	When enabled, displays the SMTP Timeout and SMTP Connection Timeout fields.
SMTP Timeout	Defines how long FortiNAC will wait if the flow of data has stalled before it fails.
SMTP Connection Timeout	Lets you define the amount of time allowed to connect to the email server before it fails.
Test Email Settings	Send a test message to the email address entered in the test settings.

Log receivers

Event and Alarm records may be stored offline on another host. The events and alarms are forwarded by using either a Syslog message or an SNMP Trap. See [Log events to an external log host on page 776](#) and [Map events to alarms on page 784](#) for more information. The host may be either an SNMP Trap receiver or a Syslog server such as FortiAnalyzer. See the [FortiAnalyzer integration guide](#) for details.

Use the Log Receivers view to add, modify, and remove external log hosts.

When the log receiver such as FortiAnalyzer is configured and added, new event and alarm logs will automatically be forwarded to the FortiAnalyzer.

Add a log host server

1. Click **System > Settings**.
2. In the tree on the left select **System Communication > Log Receivers**.
3. Click **Add** to add a log host.
4. Select the type of server.
5. Enter the **IP address** of the server.
6. Enter the configuration parameters for the type of log host. The standard port information for each host type is automatically entered. See the table below for detailed information on each type of server.
7. Click **OK**.

Settings

Field	Definition
Type	Type of server that will receive Event and Alarm messages. Options include: Syslog CSV, SNMP Trap, and Syslog Command Event Format (CEF).
IP address	IP address of the server that will receive Event and Alarm messages.
Port	Connection port on the server. For Syslog CSV and Syslog CEF servers, the default = 514. For SNMP Trap servers the default = 162
Facility	Displays only when Syslog is selected as the Type. Allows you to configure the message type. The default is 4. Options include: • 0 kernel messages • 1 user-level messages • 2 mail system • 3 system daemons • 4 security/authorization messages • 5 messages generated internally by syslogd • 6 line printer subsystem • 7 network news subsystem • 8 UUCP subsystem • 9 clock daemon • 10 security/authorization messages • 11 FTP daemon • 12 NTP subsystem • 13 log audit • 14 log alert • 15 clock daemon • 16 local use 0 (local0) • 17 local use 1 (local1) • 18 local use 2 (local2) • 19 local use 3 (local3) • 20 local use 4 (local4) • 21 local use 5 (local5) • 22 local use 6 (local6) • 23 local use 7 (local7)
Security String	Displays only when SNMP is selected as the Type. The security string sent with the Event and Alarm message.

Modify connection information

1. Click **System > Settings**.
2. In the tree on the left, select **System Communication > Log Receivers**.
3. Select a log receiver from the list and click **Modify**.

4. Edit the log host information.
5. Click **OK**.

Delete an external log host

1. Click **System > Settings**.
2. In the tree on the left select **System Communication > Log Receivers**.
3. Select a Log Receiver from the list and click **Delete**.
4. Click **Yes** on the confirmation message.

Email/SMS Message Templates

This tool allows the creation of customized message templates that are sent to notify the sponsor of incoming requests.

Steps:

1. Navigate to **System > Settings > System Communication > Email/SMS Message Templates**
2. Select **Add** to create a new template or **Modify** to edit an existing template.
3. Enter a Template Name and Email Subject.
4. Enter an HTML message in the **Message** field
5. Click **OK**.
6. Navigate to **Portal > Portal Configuration > Self Registration Login**
7. Select the template to use under **Sponsor Message Template**

Patch management

The patch management feature allows integration with patch servers such as BigFix or PatchLink. The endpoint's posture is checked on the patch servers. When an endpoint is out-of-compliance, FortiNAC automatically moves the endpoint to a separate remediation network where the patch server solution automatically updates the non-compliant system.

Settings

Field	Definition
Name	Name of the server being configured.
Type	Type of patch server, such as BigFix or PatchLink.
IP address	IP address assigned to the patch server.
Status	Indicates whether or not contact has been established between FortiNAC and the patch server.
Right click options	
Configuration (BigFix Only)	Opens a new window to modify applied actions to BigFix Baseline results.
Delete	Deletes the selected Provider. Providers that are associated with Users cannot be deleted.

Field	Definition
Properties	Displays patch management Server Properties and allows you to set the Polling Interval. Default = 2 minutes.

Servers and hosts

The Persistent Agent is required on the host to support patch management. The patch management client must also be installed on the host. If the patch management client is installed on the host the Persistent Agent reports this during its routine messages to the server.

When a patch management Server is added to the patch management View, FortiNAC queries that server to determine whether or not the host is compliant.

- If the patch management Server is not reachable, an event and alarm are generated. The host is considered compliant and remains in the production network.
 - *BigFix event* - Communication lost with the BigFix Server Database
 - *PatchLink event* - Communication lost with the PatchLink Server
- If the patch management Server is reachable and determines that the host is not compliant, the host is moved to remediation. An event is generated to indicate that the host is not compliant.
 - *BigFix events* - BigFix High Violation, BigFix Medium Violation, BigFix Low Violation
 - *PatchLink event* - PatchLink Non Compliant
- If the patch management Server is reachable and determines the host is compliant and the host was previously NOT compliant, then an event is generated to indicate that the host is now compliant. The compliant event is only generated after a not compliant event has been generated.
 - *PatchLink event* - PatchLink Compliant

Alarms can be mapped to events to notify you when the event has been generated. Each of the events listed above could be mapped to an alarm. See [Map events to alarms on page 784](#) for additional information.

PatchLink implementation

To setup communication between a PatchLink Server and FortiNAC you must do the following:

- The PatchLink NAC Integrator plug-in is required on the PatchLink server to allow PatchLink to respond to HTTP requests from FortiNAC.
- Your FortiNAC Server must have licenses for integration suite and endpoint compliance. Check the License Information panel on the dashboard to make sure you have the correct licenses. See [License management on page 983](#).
- Add the PatchLink Server to **System > Settings > System Communication > Patch Management**.
- Go to the PatchLink server properties and configure the Polling Interval. The default is 2 minutes.
- Network hosts must have the Persistent Agent installed. See [Agent overview on page 492](#).
- Network hosts must have the PatchLink Agent installed. Refer to the PatchLink documentation for instructions on installing this agent.
- Enable the PatchLink Compliant and PatchLink Non Compliant events. See [Enable and disable events on page 773](#).
- Create an Admin Scan specifically for PatchLink. These scans indicate the reason why a host was marked at risk. They are not actually scanning the host but provide a configuration or profile with which to associate the host state. Admin Scans are also used to mark hosts At Risk or Safe based on an alarm action triggered by a PatchLink event. See [Add a scan on page 616](#).

- Map alarms to the PatchLink Compliant and PatchLink Non Compliant events. For each alarm, configure a Host security action associated with the PatchLink Admin Scan earlier and mark the host At Risk or Safe depending on the alarm triggered. See [Add or modify alarm mapping on page 787](#).

PatchLink process

When PatchLink is integrated with FortiNAC as a patch management server a variety of communications occur between the two servers to make sure that hosts are compliant. The communication process is as follows:

1. The PatchLink Agent installed on the host sets a registry key value with an Agent ID value.

Example:

NameValue:

Name = PatchManagementID

Value = 6AA80EB2-CFAA-466C-9A6B-85B5A918B162

2. The FortiNAC Persistent Agent installed on the host reads the registry key and reports the value set by the PatchLink Agent back to FortiNAC. This is stored in the database, but is not displayed in the administrator Interface.
3. Based on the Polling interval set for the PatchLink server, FortiNAC gathers a list of hosts with values for PatchLink in the database and sends an HTTP request to the PatchLink server for each host. For example, if the polling interval is set to 2 minutes, then every 2 minutes an HTTP request is sent for every host in the database with PatchLink data in the host record.

Example request:

http://10.20.100.32/IntegrationPoint/EndpointSecurity_V1/Status.aspx?Agentid=A5F1D1F2-F045-4866-8903-7E920417BD62

4. The PatchLink server returns a response for each host indicating whether the host is compliant or non-compliant. For each response, either a PatchLink Compliant or a PatchLink Non Compliant event is triggered.
5. If alarms have been configured for these events, then hosts are marked either safe or at risk based on the event triggered.

Add servers

To integrate a patch management Server with FortiNAC it must be added to the patch management view.

1. Click **System > Settings > System Communication**.
2. Select **Patch Management**.
3. Click **Add**.
4. Enter a name for the server, the IP address, and select the patch server from the **Type** drop-down list.
5. Click **OK**.
6. If you select **BigFix** from the **Type** drop-down list, you are prompted to enter the BigFix database credentials, which lets FortiNAC connect directly to the data store of BigFix, allowing for BaseLine test results.



Read access is required.

PatchLink server configuration

Once the PatchLink server has been added to the Topology, the polling interval must be entered into the properties view. The polling interval is the length of time FortiNAC will wait before polling the PatchLink Server for updated client status information.

1. Click **Network > Inventory** and expand the **FortiNAC** and **Patch Management** icons.
2. Right-click on the **PatchLink Server** and select **Properties**.
3. Enter the polling interval.
4. Click **Apply**.

BigFix server properties

Once the BigFix patch management server has been added to the patch management Servers view, the connection parameters for the server and database must be entered to allow FortiNAC to communicate with the server and database.



The Persistent Agent must be installed to communicate with a patch management integration.



The BigFix Client must be installed and be connected to the BigFix Server before the Persistent Agent is installed.

1. Click **System > Settings > System Communication > Patch Management**.
2. Right-click on the **BigFix Patch Management Server** and select **Properties**.
3. Use the table below to enter the connection parameters for the server and database.
4. Click **The BigFix Client must be installed and be connected to the BigFix Server before the Persistent Agent is installed.**

Settings

Field	Description
Database IP	The IP address of the server where the database resides.
Database Port	The port on the server used for access to the database information.
Database Name	The name of the database.
Database User	The username used to access the database information.
Database Password	The password for access to the database for the entered database user.
Polling Interval (Sec)	The length of time between polls to the patch management server to retrieve data.
Test Connection	Allows you to test SQL Server credentials for patch management servers.

Once communication with the BigFix patch management server has been established the Administrator will use the BigFix server's Configuration view to view the status of host endpoint systems and select an action to take if the host is out of compliance.

BigFix configuration

The Configuration view contains a list of the Base-Line Names from the BigFix server. Each of the Base-Line Names has an associated Failure Action and Untested Action.

Although actions applied will affect all users that report as failed or untested, the report will only show online users being affected.

Field	Description
Base-Line Name	A list of required patches given in the BigFix database that the host must have to be in compliance. The list of hosts or groups that the Base-Line Name apply to are determined in the BigFix server.
Failure Action	The action that can be applied to an endpoint if it has failed the test for the Base-Line Name indicated.
Untested Action	The action that can be applied to an endpoint if it has not been tested against the Base-Line Name indicated.

The administrative action is an Admin scan that is created in Remediation Configuration. See [Remediation configurations on page 615](#) for details on adding and using an Admin scan.

Admin scans must be created under Remediation Configuration before you can select them here. See [Remediation configurations on page 615](#).

To apply a **Failure** or **Untested** action on an endpoint:

1. Click **System > Settings > System Communication > Patch Management**.
2. Right-click on the **BigFix Patch Management Server** and select **Configuration**.
3. Select the **Severity** under **Failure Action** to apply that action to the hosts indicated in the **Base-Line Name** that have failed to meet the specified patch requirements.
4. Select the **Severity** under **Untested Action** to apply that action to the hosts indicated in the **Base-Line Name** that have not been tested to determine whether or not the specified patch requirements have been met.
5. Click **Apply**.



The severity creates an alarm that can be associated with actions, including Admin Scans. See [Map events to alarms on page 784](#)

In **Logs > Events & Alarms > Mappings**, three events can be used for security related actions:

- BigFix Low Violation
- BigFix Medium Violation
- BigFix High Violation

When creating these events, an action may be applied to accompany the creation of the alarm. To use Admin Scans created in the Remediation Configuration, do the following:

1. Select **Host Security Action**.
2. Select the **Admin Scan** for which the host state will be modified.



When applying a severity to results of a baseline action, the online hosts that are affected will be in the Baseline Host Report. To access this report, select **Hosts** next to the severity being applied.

BigFix Baseline Host

The data displays hosts that are currently online that have reported as untested or failed by BigFix.



These host reports only display online users. However, the action applied will affect all users who have a Persistent Agent and a BigFix Client installed simultaneously.

Proxy settings

Proxy settings allows you to configure FortiNAC Manager to direct web traffic to a proxy server in order to download OS updates and auto-definition updates.

Proxy communication is not supported for MDM Services.

FortiNAC Manager Requirement: If proxy is enabled, both the FortiNAC Manager and managed FortiNAC CA servers must have their subnet(s) for port1/eth0 or domain(s) listed in the exclusions list. See Proxy Exclusions in the table below.

1. Click **System > Settings**.
2. Expand the System Communication folder.
3. Select **Proxy Settings** from the tree.
4. Use the table below to enter the necessary settings.
5. Click **Save Settings**.

Field	Definition
Enable Proxy Configuration	If enabled, FortiNAC Manager will use the Proxy Configuration to download OS updates and auto-definition updates.
Host	The hostname or address of the proxy server. Note: When using the hostname, verify FortiNAC can resolve the name prior to enabling Proxy Settings. Due to DNS caching, traffic may not be properly forwarded to the proxy server for a period of time once the name is reachable. If this occurs, disable and re-enable Proxy Settings. See article https://community.fortinet.com/t5/FortiNAC-F/Technical-Tip-FortiNAC-cannot-reach-FortiCloud-in-a-proxy/ta-p/433486
Port	Port used for communication with the proxy server. This must match the port setting on the proxy server itself.
Authentication	If enabled, you must enter the user name and password for the proxy server.
User Name	User Name for the email account used as the sender account.

Field	Definition
Password	Password for the email account used as the sender account.
Use HTTP Proxy settings for all protocols	If enabled, the HTTP Proxy configuration will be used for both HTTPS and FTP Proxy communication.
Proxy Exclusions	Indicates the hosts that should be accessed without going through the proxy. This is a required setting for FortiNAC Manager and the managed FortiNAC CA servers if proxy is enabled. Server synchronization between FortiNAC Manager and FortiNAC CA uses REST API. The Proxy Exclusion configuration prevents REST calls between the Manager and the CA from redirecting to the proxy server. If these calls are sent to the proxy, the synchronization process will not complete. The list of hosts are separated by the ' ' character. The wildcard character '*' can be used at the beginning or end of the string for pattern matching (e.g., *.foo.com localhost" indicates that every host in the foo.com domain and the localhost should be accessed directly, even if a proxy server is specified). Note: Using wildcard in the middle of the string is not supported (e.g. myhost.*.foo.com) Required for FortiNAC Manager and managed CA servers: Include the port1/eth0 IP addresses, subnets or domains of the managed FortiNAC CA servers and Manager. Example FortiNAC Manager Port1/eth0 IP: 10.10.10.4/24 Domain name: NACMgr.myntwk.com FortiNAC CA Port1/eth0 IP's: 10.10.10.5/24, 10.10.20.5/24 Domain names: NAC10.myntwk.com, NAC20.myntwk.com One of the following examples would be entered in the Proxy Exclusions list of the Manager, NAC10 and NAC20: A) 10.10.10.* 10.10.20.* B) 10.10.10.4 10.10.10.5 10.10.20.5.10 C) *.myntwk.com D) FortiNAC Managergr.myntwk.com NC10.myntwk.com NC20.myntwk.com

SSH Key Management

SSH Key Management allows generation and management of SSH key. These SSH keys allow FortiGate integration through establishing secure communication between FortiNAC and FortiGate without the need for password-based logins by deploying the SSH keys onto FortiGate devices.

SSH Key management is located at **System > Settings > System Communication > SSH Key Management**.

The SSH key Management can generate various types of SSH keys, store these keys in database, delete them, and show which key is being used by FortiGate.

Types of SSH keys

These are the algorithms that SSH key management supports:

- RSA
- ECDSA (256-bit)
- ECDSA (384-bit)
- ECDSA (521-bit)
- Ed25519

Generation of SSH Key

These steps shows how to generate a new SSH key

1. Go to **System > Settings > System Communication > SSH Key Management**.
2. Click **Generate** to generate a new SSH key.
3. Click **Type** drop down menu to select a SSH Key type.
4. Name the SSH Key, and click **OK**.

After the SSH Key is generated, it can be added onto the device credentials of FortiGate. Go to **Network > Inventory > select a FortiGate device > Credentials** to select the SSH key. See [Credentials on page 351](#) for more details

Look up usage of SSH Key

1. Click on a SSH key.
2. Click **Used By** to see which device the SSH key is being used.

Verify the SSH key used on FortiGate through FortiGate CLI

After the SSH key is attached to the FortiGate machine through the FortiGate device Credential settings. It can be verified through FortiGate CLI.

1. Log in FortiGate CLI as admin.
2. Enter the following CLI commands to show the SSH public key:

```
config system admin
show
```

SSH Key Management through CLI

SSH Key management can be done through FortiNAC CLI- `execute ssh-authentication-keys`. This SSH command allows you to generate, list, and remove SSH public keys. For more details please see [Execute commands](#)

under the SSH section.

SNMP

Use the SNMP Properties view to select the SNMP protocol for devices that query FortiNAC for information. If SNMP is enabled, FortiNAC responds to SNMP communication from other devices, such as a Network Management system that might include the FortiNAC server in its own database.



FortiNAC-OS Requirement: "snmp" option must be included in the "set allowaccess" command. See [Open ports](#) for details.

Go to **Settings > System Communication > SNMP**.

In addition, this view is also used to set the SNMP protocol to accept SNMPv3 traps that register hosts and users.

Both types of communication pass through port 161. Settings here are global. Therefore, if you choose to use SNMPv3 traps sent from other network devices to register hosts and users, then ALL other devices that query FortiNAC for information must also communicate using SNMPv3. You must modify the configuration of those external devices to use SNMPv3.

The SNMP protocols that are supported are SNMPv1/SNMPv2c and SNMPv3. SNMPv3 uses DES or AES encryption for the Privacy Password.

Privacy protocols supported are:

- DES
- Triple-DES
- AES-128

SNMP MIBs used to communicate with FortiNAC are in: `/bsc/campusMgr/ui/runTime/docs/mibs/`

See [FortiNAC MIB's](#).

Settings

Field	Description
Enable SNMP Communication	If SNMP is enabled, FortiNAC responds to SNMP requests from other servers.
SNMP Protocol	Select the SNMP protocol FortiNAC will be responding to: • SNMPv1/SNMPv2c • SNMPv3-AuthPriv (SNMPv3 with authentication and privacy) • SNMPv3 AuthNoPriv (SNMPv3 with authentication but no privacy.)
SNMPv1/SNMPv2c	
Security String	Enter the security string that FortiNAC will respond to when communicating with the server.
SNMPv3	

Field	Description
User Name	User Name for the SNMPv3 credentials.
Authentication Protocol	Specify the SNMPv3 authentication protocol. The available authentication protocols are: • MD5 • SHA1
Authentication Password	Specify the authentication password required by FortiNAC when SNMPv3-AuthPriv or SNMPv3-AuthNoPriv queries are received.
Privacy Protocols	Specify the SNMPv3 privacy protocol. The available privacy protocols are: • DES • Triple-DES • AES-128
Privacy Password	Specify the privacy password required by FortiNAC when SNMPv3-AuthPriv queries are received.
Management hosts	
IP addresses	List of IP addresses of the devices that have communicated with FortiNAC through SNMP.

Set up SNMP communication

1. Click **System > Settings**.
2. Expand the **System Communication** folder.
3. Select **SNMP** from the tree.
4. Click **Enable** and select an **SNMP protocol**.
5. Enter the **parameters** as required for the selected protocol. See the table above for additional information.
6. Click **Save Settings**.

Disable SNMP communication

1. Click **System > Settings**.
2. Expand the **System Communication** folder.
3. Select **SNMP** from the tree.
4. Click **Disable**.
5. Click **Save Settings**.

Register hosts and users with SNMPv3 traps

FortiNAC can use data sent in SNMPv3 traps from external devices to register hosts and users. This speeds up the process of adding hosts and users to your FortiNAC database by taking advantage of information that is readily available from another system. In addition, based on trap parameters hosts and users can be modified or removed from the database.

FortiNAC requirements

- FortiNAC must have an integration suite license. See [Licenses on page 29](#).
- The Trap Sender must be modeled in the Inventory as a pingable device. See [Add or modify a pingable device on page 302](#).
- You must enter SNMPv3 settings in **System > Settings > System Communication > SNMP** that match those of the device to which you are sending traps. Note that if you had previously entered SNMPv1/SNMPv2c settings for external devices querying FortiNAC for information, you must modify settings on those devices to use SNMPv3.
- If you are running FortiNAC in a FortiNAC Manager environment, the Trap Sender must be modeled on each FortiNAC Server that should receive this information. Note that if you have enabled any of the **Copy Registered Host** options on the FortiNAC Manager it may not be necessary to receive traps on more than one managed server.
- When traps are received they can trigger the events listed below in the Event Log. These events can be mapped to Alarms. Make sure the events are enabled. See [Event management on page 772](#). To map events to alarms see [Add or modify alarm mapping on page 787](#).

Event	Definition
Add/Modify/Remove Host	Generated whenever a trap is received that adds, modifies or removes a host record in the database.
Add/Modify/Remove User	Generated when a trap is received that adds, modifies or removes a user record in the database.

Trap sender requirements

- Use the Management IP address (port1) of the FortiNAC Server as the destination for the trap.
- Send traps to port 161 on the FortiNAC Server.
- If you are running FortiNAC in a high availability environment, send traps to both the primary and the secondary FortiNAC Servers.
- You must have snmptrap.exe and libsnmp.dll on the device sending the traps. Download the latest binaries for the appropriate operating system from www.net-snmp.org/download.html.
- Configure the traps on the sending device. See the tables below for information on trap parameters.

Hosts

- If a trap is received for an existing host, the host's database record is updated with information from the trap.
- When a trap is received for a host that matches a rogue in FortiNAC, the rogue is converted to a registered host if the trap contains user data. It is converted to a registered device if there is no associated user.
- If a user is deleted based on a trap, associated hosts are not deleted and they become registered devices. To delete these hosts either send an additional trap that removes the host or you must go to the Host View and delete them manually. See [Delete a host on page 229](#).
- If the same host is added twice but with different MAC addresses for separate adapters, it is treated as two separate records in the FortiNAC database. The two adapters are not linked to each other in any way and are not considered siblings in FortiNAC.
- Variables with spaces in the names should be in quotation marks, such as "Windows Vista".
- Separators in MAC addresses must be colons, such as 90:21:55:EB:A3:87.

OID	Description	Definition
1.1.1.1	Host Name	Name of the host.
1.1.1.2	IP address	IP address of the host.
1.1.1.3	MAC address	Physical Address of the host. Required.
1.1.1.4	Host operating system	Name of the operating system on the host.
1.1.5	Role	Role assigned to the host. Roles are attributes of hosts used as filters in user/host profiles.
1.1.6	Action	Indicates whether this trap is adding or removing a host from the database. Adding an existing host will modify that host's record in the database. 1=Add 2=Remove
1.2.8	Element	Indicates that this trap is registering either a host or a host and its corresponding user.

Example traps

To add a host record for the PC with a hostname of *Gateway-notebook*, with an IP address of *160.87.100.117*, a MAC address of *00:26:9E:E2:DD:DB*, an OS of *Windows*, and a role of *Guest*:

```
snmptrap -v3 -u <user**> -l authNoPriv -a MD5 -A <Passphrase**> 160.87.9.10:161 ''
1.3.6.1.4.1.16856.1.2.8 .1.3.6.1.4.1.16856.1.1.1.1 s Gateway-notebook
.1.3.6.1.4.1.16856.1.1.1.4 s Windows .1.3.6.1.4.1.16856.1.1.1.2 s 160.87.100.117
.1.3.6.1.4.1.16856.1.1.1.3 s 00:26:9E:E2:DD:DB .1.3.6.1.4.1.16856.1.1.5 s Guest
.1.3.6.1.4.1.16856.1.1.6 integer 1
```

To remove host record for the PC with a hostname of *Gateway-notebook*, with an IP address of *160.87.100.117*, a MAC address of *00:26:9E:E2:DD:DB*, an OS of *Windows*, and a role of *Guest*. Note that only MAC address is required to remove a host.

```
snmptrap -v3 -u <user**> -l authNoPriv -a MD5 -A <Passphrase**> 160.87.9.10:161 ''
1.3.6.1.4.1.16856.1.2.8 .1.3.6.1.4.1.16856.1.1.1.1 s Gateway-notebook
.1.3.6.1.4.1.16856.1.1.1.4 s Windows .1.3.6.1.4.1.16856.1.1.1.2 s 160.87.100.117
.1.3.6.1.4.1.16856.1.1.1.3 s 00:26:9E:E2:DD:DB .1.3.6.1.4.1.16856.1.1.5 s Guest
.1.3.6.1.4.1.16856.1.1.6 integer 2
```

Users

- If an LDAP directory is modeled in the Inventory, FortiNAC checks the directory for information about the user included in the trap. If the user exists in the directory, additional fields are populated for that user in the FortiNAC database. If the user does not exist in the directory, a user record is created in FortiNAC with only the data received in the trap.
- If a trap is received for an existing user, the user's database record is updated with information from the trap.
- If a trap is received for an existing user and the trap contains host information, the host is registered to the user. If the host already has a rogue record, the rogue is converted to a registered host and associated with the user.
- If a user is deleted based on a trap, associated hosts are not deleted and they become registered devices. To delete these hosts you must go to the Host View and delete them manually. See [Delete a host on page 229](#).

- When FortiNAC resynchronizes with the directory, user data may be overwritten by data from the directory depending on the directory attribute mappings.
- Variables with spaces in the names should be in quotation marks, such as "Mary Ann".

Trap parameters

OID	Description	Definition
1.1.2.1	User Name	User Name stored in the directory. If the user is not in the directory, this record will still be added, modified or removed. Required.
1.1.2.2	User First Name	
1.1.2.3	User Last Name	
1.1.2.4	User Title	
1.1.2.5	Email	User's e-mail address.
1.1.5	Role	Role assigned to the User. If this trap is adding both a user and a host, both are set to the same role.
1.1.6	Action	Indicates whether this trap is adding or removing a user from the database. Adding an existing user will modify that user's record in the database. 1=Add 2=Remove
1.2.9	Element	Indicates that this trap is only registering a user.

Example traps

To add `testuser` to the database:

```
snmptrap -v3 -u <user**> -l authNoPriv -a MD5 -A <Passphrase**> 160.87.9.10:161 ''
1.3.6.1.4.1.16856.1.2.9 .1.3.6.1.4.1.16856.1.1.2.1 s testuser
.1.3.6.1.4.1.16856.1.1.2.2 s John.1.3.6.1.4.1.16856.1.1.2.3 s Doe
.1.3.6.1.4.1.16856.1.1.2.4 s Mr .1.3.6.1.4.1.16856.1.1.2.5 s jdoe@megatech.com
.1.3.6.1.4.1.16856.1.1.5 s Guest .1.3.6.1.4.1.16856.1.1.6 integer 1
```

To delete user record for `testuser` from the database. Note that only User Name is required to remove a user.

```
snmptrap -v3 -u <user**> -l authNoPriv -a MD5 -A <Passphrase**> 160.87.9.10:161 ''
1.3.6.1.4.1.16856.1.2.9 .1.3.6.1.4.1.16856.1.1.2.1 s testuser
.1.3.6.1.4.1.16856.1.1.2.2 s John.1.3.6.1.4.1.16856.1.1.2.3 s Doe
.1.3.6.1.4.1.16856.1.1.2.4 s Mr .1.3.6.1.4.1.16856.1.1.2.5 s jdoe@megatech.com
.1.3.6.1.4.1.16856.1.1.5 s Guest .1.3.6.1.4.1.16856.1.1.6 integer 2
```

FortiNAC MIBs

If SNMP is enabled under the SNMP Properties view, FortiNAC responds to SNMP communication from other devices, such as a Network Management system that might include the FortiNAC server in its own database.

Important: FortiNAC-OS Requirement: "snmp" option must be included in the "set allowaccess" command. See Open ports for details.

The following SNMP MIBs are used to communicate with FortiNAC. They are also documented in the FortiNAC system under the directory `/bsc/campusMgr/ui/runTime/docs/mibs/`.

Hardware

OID	Description
enterprises.16856	The FortiNAC MIB
1.4.1.1.0	cpuDescription OBJECT-TYPE SYNTAX DisplayString MAX-ACCESS read-only STATUS current DESCRIPTION "Textual description of CPU." ::= { hardware 1 }
1.4.1.2.0	cpuCount OBJECT-TYPE SYNTAX Integer32 MAX-ACCESS read-only STATUS current DESCRIPTION "The number of CPUs." ::= { hardware 2 }
1.4.1.3.0	cpuCache OBJECT-TYPE SYNTAX Integer32 MAX-ACCESS read-only STATUS current DESCRIPTION "The CPU cache in kbytes." ::= { hardware 3 }
1.4.1.4.0	osVersion OBJECT-TYPE SYNTAX DisplayString MAX-ACCESS read-only STATUS current DESCRIPTION "Textual description of operating system." ::= { hardware 4 }
1.4.1.5.0	databaseVersion OBJECT-TYPE SYNTAX DisplayString MAX-ACCESS read-only STATUS current DESCRIPTION "Textual description of database version." ::= { hardware 5 }

OID	Description
1.4.1.6.0	webVersion OBJECT-TYPE SYNTAX DisplayString MAX-ACCESS read-only STATUS current DESCRIPTION "Textual description of web server version." ::= { hardware 6 }
1.4.1.7.0	totalMemory OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "Total memory (kbytes)." ::= { hardware 7 }
1.4.1.8.0	freeMemory OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "Free memory (kbytes)." ::= { hardware 8 }
1.4.1.9.0	totalSwap OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "Total swap (kbytes)." ::= { hardware 9 }
1.4.1.10.0	freeSwap OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "Free swap (kbytes)." ::= { hardware 10 }
1.4.1.11.0	totalDisk OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "Total disk (kbytes)." ::= { hardware 11 }

OID	Description
1.4.1.12.0	freeDisk OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "Free disk (kbytes)." ::= { hardware 12 }

Software

OID	Description
enterprises.16856	The FortiNAC MIB
1.4.2.1.0	concurrentLicenseCount OBJECT-TYPE SYNTAX Integer32 MAX-ACCESS read-only STATUS current DESCRIPTION "The number of concurrent licenses." ::= { software 1 }
1.4.2.2.0	concurrentLicensesUsed OBJECT-TYPE SYNTAX Integer32 MAX-ACCESS read-only STATUS current DESCRIPTION "The number of concurrent licenses used." ::= { software 2 }

Client

OID	Description
enterprises.16856	The FortiNAC MIB
1.4.3.1.0	totalClients OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of managed clients in the system." ::= { client 1 }

OID	Description
1.4.3.2.0	registeredCount OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of registered clients in the system." ::= { client 2 }
1.4.3.3.0	registeredOnLineCount OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of registered clients on line in the system." ::= { client 3 }
1.4.3.4.0	registeredOffLineCount OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of registered clients off line in the system." ::= { client 4 }
1.4.3.5.0	rogueCount OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of unregistered clients in the system." ::= { client 5 }
1.4.3.6.0	rogueOnLineCount OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of unregistered clients on line in the system." ::= { client 6 }
1.4.3.7.0	rogueOffLineCount OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of unregistered clients off line in the system." ::= { client 7 }

OID	Description
1.4.3.8.0	disabledCount OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of disabled clients in the system." ::= { client 8 }
1.4.3.9.0	disabledOnLineCount OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of disabled clients on line in the system." ::= { client 9 }
1.4.3.10.0	disabledOffLineCount OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of disabled clients off line in the system." ::= { client 10 }
1.4.3.11.0	atRiskCount OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of at risk clients in the system." ::= { client 11 }
1.4.3.12.0	atRiskOnLineCount OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of at risk clients on line in the system." ::= { client 12 }
1.4.3.13.0	atRiskOffLineCount OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of at risk clients off line in the system." ::= { client 13 }

OID	Description
1.4.3.14.0	userCount OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of managed users in the system." ::= { client 14 }
1.4.3.15.0	userOnLineCount OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of managed users on line in the system." ::= { client 15 }
1.4.3.16.0	userOffLineCount OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of managed users off line in the system." ::= { client 16 }
1.4.3.17.0	ipPhoneCount OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of IP Phones in the system." ::= { client 17 }
1.4.3.18.0	ipPhoneOnLineCount OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of IP Phones on line in the system." ::= { client 18 }
1.4.3.19.0	ipPhoneOffLineCount OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of IP Phones off line in the system." ::= { client 19 }

Device

OID	Description
enterprises.16856	The FortiNAC MIB
1.4.4.1.0	totalDevices OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of managed devices in the system." ::= { device 1 }
1.4.4.2.0	routerCount OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of routers in the system." ::= { device 2 }
1.4.4.3.0	routerON OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of routers on line in the system." ::= { device 3 }
1.4.4.4.0	routerOFF OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of routers off line in the system." ::= { device 4 }
1.4.4.5.0	switchCount OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of wired switches in the system." ::= { device 5 }

OID	Description
1.4.4.6.0	switchON OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of wired switches on line in the system." ::= { device 6 }
1.4.4.7.0	switchOFF OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of wired switches off line in the system." ::= { device 7 }
1.4.4.8.0	wswitchCount OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of wireless switches in the system." ::= { device 8 }
1.4.4.9.0	wswitchON OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of wireless switches on line in the system." ::= { device 9 }
1.4.4.10.0	wswitchOFF OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of wireless switches off line in the system." ::= { device 10 }
1.4.4.11.0	hubCount OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of hubs in the system." ::= { device 11 }

OID	Description
1.4.4.12.0	hubON OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of hubs on line in the system." ::= { device 12 }
1.4.4.13.0	hubOFF OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of hubs off line in the system." ::= { device 13 }
1.4.4.14.0	serverCount OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of servers in the system." ::= { device 14 }
1.4.4.15.0	serverON OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of servers on line in the system." ::= { device 15 }
1.4.4.16.0	serverOFF OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of servers off line in the system." ::= { device 16 }
1.4.4.17.0	printerCount OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of printers in the system." ::= { device 17 }

OID	Description
1.4.4.18.0	printerON OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of printers on line in the system." ::= { device 18 }
1.4.4.19.0	printerOFF OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of printers off line in the system." ::= { device 19 }
1.4.4.20.0	interfaceCount OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of interfaces in the system." ::= { device 20 }
1.4.4.21.0	interfaceON OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of interfaces on line in the system." ::= { device 21 }
1.4.4.22.0	interfaceOFF OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of interfaces off line in the system." ::= { device 22 }
1.4.4.23.0	uplinkCount OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of up links line in the system." ::= { device 23 }

OID	Description
1.4.4.24.0	userDefinedUplinkCount OBJECT-TYPE SYNTAX Counter32 MAX-ACCESS read-only STATUS current DESCRIPTION "The total number of user defined up links in the system." ::= { device 24 }

Syslog files



FortiNAC-OS Requirement: "syslog" option must be included in the "set allowaccess" command. See [Open ports](#) for details.

You can choose to send output from IPS/IDS devices to FortiNAC. Syslog Files that you create and store under Syslog Management are used by FortiNAC to parse the information received from these external devices and generate an event. The event can contain any or all of the fields contained in the syslog output.

Default files

Default files include:

- FireEye
- FortiOS4
- FortiOS5
- Palo Alto Networks Firewall
- Sourcefire IPS
- StoneGate IPS
- TippingPoint SMS
- Top Layer IPS

Each of these files has corresponding events in the events list. You can add configurations for other Syslog files if they conform to either the CSV, CEF or TAG/VALUE formats.

Events and alarms

When those new Syslog configurations are added, corresponding events and alarms are created in the Events List. See [Events and alarms list on page 750](#) for a complete list of events that can be tracked.

If a syslog message is received for a host that has more than one adapter, an event is generated for each adapter. Therefore a single host could generate multiple events and alarms.

Device model

You must model any device that sends Syslog information to FortiNAC in the Inventory. See [Add or modify a pingable device on page 302](#) for detailed instructions.

Navigation

To access the **Syslog Management** view, select **System > Settings > System Communication > Syslog Files**.

Settings

Field	Definition
Table configuration	
Enable Buttons	Enables or disables the selected Syslog file. If a file is disabled it is not used when processing inbound syslog messages.
Table columns	
Name	The name of the syslog file. This is a unique name for this syslog definition. This value is required.
Enabled	A green check mark indicates that the file is enabled. A red circle indicates that the file is disabled.
Label	The label for the Event or Alarm that will be generated. This value is required.
Format	Message format for the Syslog file. Supported formats include: • CSV: Message is a series of data fields typically separated by commas. Comma separated value. Other characters can be used to separate data fields. • TAG/VALUE: Message is series of fields each with a tag and a value. For example, the message could contain the following : cip=192.168.10.182. cip is the tag indicating that this is the IP address of the user causing the problem. 192.168.10.182 is the value associated with that tag. • CEF: Message is a series of fields, some in a standard position, others with a tag and a value. For example the message could contain the following: src=192.168.10.182. src is the tag indicating that this is the IP address of the user causing the problem. 192.168.10.182 is the value associated with that tag.
Delimiter	Character used to separate the fields in the syslog message. Options include: space, comma (,) and pipe (). This field is not available for the TAG/VALUE format. A space is used as the delimiter.
IP Tag/Column	Name of the field or number of the column containing the source IP address. This value is required.
Filter Tag/Column	Name of the field or number of the column containing the filter. This value is required.
Filter Value	The value contained in the filter column or field. Only entries that contain matching data will be used. This value is required.
Severity Tag/Column	Name of the field or number of the column containing the severity. This value is required.

Field	Definition
Low Severity Values	Entries containing one of these matching values in the severity field or column cause a Low Severity event to be generated. For CSV format, multiple values are entered separated by commas.
Medium Severity Values	Entries containing one of these matching values in the severity column will cause a Medium Severity event to be generated. For CSV format, multiple values are entered separated by commas.
High Severity Values	Entries containing one of these matching values in the severity field or column cause a High Severity event to be generated. For CSV format, multiple values are entered separated by commas.
Event Tag/Column	Names of the fields or numbers of the columns used when populating items from the syslog entry into the Event Format.
Event Format	Message that is displayed when the event is generated. The text is generated from the items listed in the Event Tag field in the order they appear.
Right click options	
Add	Opens the Add Syslog Files dialog.
Delete	Deletes the selected action.
Modify	Opens the Modify Security Action window for the selected action.
In Use	Shows if the Syslog File is in use or not
Show Audit Log	Opens the admin auditing log showing all changes made to the selected item. For information about the admin auditing log, see Audit Logs on page 746.  You must have permission to view the admin auditing log. See Add an administrator profile on page 139.
Enable	Enables the syslog file.
Disable	Disables the syslog file.

Inbound file formats

There are three supported syslog formats, CSV, TAG/VALUE and CEF. The CSV syslog output format is a comma-separated entry with seven items. Identify each item in the entry by its column number when you create the Event Message format. The TAG/VALUE syslog output format is a set of messages where the TAG indicates the name of the program or process that generated the message and the VALUE is the content of the message. The CEF syslog output format uses tags to mark the data so that it can be located by the device receiving the syslog file.

Example:

```
Denied,10,192.168.1.1,00:10:8B:A7:EF:AA,IPS Sensor,214,P2P-TCP-BitTorrent-Network-Connect
```

Column Number	Description	Data From Example
1	Action taken by IPS/IDS	Denied
2	Alert Severity	10
3	Source IP address	192.168.1.1
4	Source MAC address	00:10:8B:A7:EF:AA
5	Component ID	IPS Sensor
6	Rule ID	214
7	Situation	P2P-TCP-BitTorrent-Network-Connect

Example:

```
<38>Apr 14 09:48:55 192.168.5.199 IPS5500-1000: id=060001 pt=TLN-TM prot=TCP
cip=192.168.10.182 cpvt=49161 sip=192.168.10.10 spvt=445 atck=tlN-001017
disp=mitigate ckt=1 src=extern msg="NETWK: TCP Connection With Missed Setup"
```



Only the fields used by Syslog Management are defined in the table.



Values within the TAG/VALUE syslog must not contain spaces, unless the value is contained within double-quotes ("), such as msg="NETWK: TCP Connection With Missed Setup."

TAG Name	Description	VALUE From Example
cip	IP address of the host	192.168.10.182
prot	Protocol	TCP
atck	Filter - severity	tlN-001017
TLN-	Filter	tlN-
msg	Message	"NETWK: TCP Connection With Missed Setup"

Example:

```
CEF:0|FireEye|MPS|5.1.0.55701|MC|malware-callback|9|src=195.2.252.157 spt=80
smac=00:0d:66:4d:fc:00 rt=May 08 2010 14:24:45 dst=128.12.95.64 dpt=0
dmac=00:18:74:1c:a1:80 cn1Label=vlan cn1=0 cn2Label=sid cn2=33331600 cs1Label=sname
cs1=Trojan.Piptea.2 msg= https://mil.fireeye.com/edp.php?sname\=Trojan.Piptea.2
cs4Label=link cs4= https://172.16.127.7/event_stream/events?event_id\=111
cs5Label=ccName cs5=195.2.252.157 cn3Label=ccPort cn3=80 proto=tcp shost=rescomp-
09-149735.Standard.EDU dvcHost=mslms dvc=172.16.127.7 externalId=111
```

The first part of the message has a common format and is not tagged. It follows the format shown below. Other fields are customized.

CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension



This only an example and does not list all of the possible combinations of data that can be used to generate events and alarms.

TAG Name	Description	VALUE From Example
src	IP address of the host	195.2.252.157
Severity	Severity	9
Name	Event Name	malware-callback
proto	Transport Protocol	tcp
cs1	Signature Name	Trojan Piptea 2

Add or modify a syslog file

Refer to for file format information.



The asterisk (*) wildcard can be used at the beginning and end of all values you enter.

1. Click **System > Settings**.
2. Select **Syslog Files** from the tree.
3. Click **Add** or select an existing Syslog File from the list and click **Modify**.
4. Check the **Processing Enabled** check box to enable this Syslog file.
5. Enter a **Name** for the Syslog File.
6. Use the table below to enter the file information.
7. Click **OK** to save the new Syslog file.
8. You need to add the IDS/IPS device if it is not already in the Inventory. See [Add or modify a pingable device on page 302](#) for detailed instructions.

Settings



All possible fields are shown in the table. Fields on the Add or Modify dialog will vary depending on whether you chose CSV or TAG/VALUE format.

Field	Definition
Name	The name of the syslog file. This is a unique name for this syslog definition. This value is required.

Field	Definition
Processing Enabled	Enables/disables processing of this type of inbound syslog messages.
Event Label	The label for the Event or Alarm that will be generated by FortiNAC. This value is required.
Format	Supported message formats include: • CSV: Message is a series of data fields typically separated by commas. Comma separated value. Other characters can be used to separate data fields. • TAG/VALUE: Message is series of fields each with a tag and a value. For example, the message could contain the following: <code>cip=192.168.10.182</code>. <code>cip</code> is the tag indicating that this is the IP address of the user causing the problem. <code>192.168.10.182</code> is the value associated with that tag. • CEF: Message is a series of fields, some in a standard position, others with a tag and a value. For example the message could contain the following: <code>src=192.168.10.182</code>. <code>src</code> is the tag indicating that this is the IP address of the user causing the problem. <code>192.168.10.182</code> is the value associated with that tag.
IP Tag IP Column	Name of the field or number of the column containing the source IP address. This value is required.
Filter Tag Filter Column	Name of the field or number of the column containing the filter.  This value is required. If left blank, there will be no matches and no syslog data is sent to FortiNAC.
Filter Values	The values contained in the filter column or field. Only entries that contain matching data will be used. This value is required. If left blank, everything is a match.
Severity Tag/Column	Name of the field or number of the column containing the severity. This value is required.
Severity Values	Entries containing one of these matching values in the severity field or column cause a Low, Medium or High Severity event to be generated. For CSV format, separate values with commas if entering more than one possible value.
Event Tag Event Column	The names of the fields or numbers of the columns used when populating items from the syslog entry into the Event Format.
Entire Syslog	Insert <code>%syslog%</code> as an event column in the location where you want the syslog message to appear in the event.
Event Format	Message that is displayed when the event is generated. The text is generated from the items listed in the event tag parameter in the order they appear.

Delete a syslog file

1. Click **System > Settings**.
2. Expand the **System Communication** folder.

3. Select **Syslog Files** from the tree.
4. Select the file to delete and click **Delete**.
5. The program asks if you are sure. Click **Yes** to continue.

Examples of syslog messages

Here are some examples of syslog messages that are returned from FortiNAC. In these examples, the Syslog server is configured as follows:

- Type: Syslog
- IP address: a.b.c.d
- Port: 514
- Facility: Authorization

Event	Description	Syslog Message
Login Success	This is the event that is logged with a user logs into the admin UI.	02-28-2014 08:16:04 Auth.Notice 192.168.34.31 Feb 27 22:16:14 : 2014/02/27 22:16:14 EST,1,545570,Login Success,0,12,,,,,User root logged in.
Map IP To MAC Failure	This is a legacy event logged when a scheduled task runs (these are no longer used for IP-MAC) and the ARP is not read.	--
Probe - Map IP To MAC Failure	This is the event when we fail to poll and L3 device for IP->MAC (reading Arp Cache) L3 Polling	02-28-2014 09:00:14 Auth.Notice 192.168.34.31 Feb 27 23:00:24 : 2014/02/27 23:00:24 EST,1,545702,Probe - MAP IP To MAC Failure,0,28,,Switch,192.168.34.1,,Failed to read IP address mappings from device Switch.
User Logged Out	This is the event that is logs when a user logs out of the admin UI.	02-28-2014 08:48:55 Auth.Notice 192.168.34.31 Feb 27 22:49:04 : 2014/02/27 22:49:04 EST,1,545670,User Logged Out,0,12,,,,,User root Logged Out.
User Logged off Host	This event is logged when a user logs off a host	02-28-2014 08:44:25 Auth.Notice 192.168.34.31 Feb 27 22:44:34 : 2014/02/27 22:44:34 EST,1,545655,User Logged off Host,0,4155,,,,,"User Man, Bat logged off session 1 on host BRADSUPP7-LT"
User Logged onto Host	This event is logged when a user logs onto a host	02-28-2014 08:37:58 Auth.Notice 192.168.34.31 Feb 27 22:38:07 : 2014/02/27 22:38:07 EST,1,545633,User Logged onto Host,0,4155,,,,,"User Man, Bat logged onto session 1 on host BRADSUPP7-LT"

Event	Description	Syslog Message
User Remotely Connected to Host	An event that is logged when a user remotely connected to a terminal session on a host using the PA	--
User Locked Session	This event is logged when a user locks his workstation	02-28-2014 08:49:53 Auth.Notice 192.168.34.31 Feb 27 22:50:03 : 2014/02/27 22:50:03 EST,1,545681,User Locked Session,0,4155,,,,,"User Man, Bat locked session 2 on host BRADSUPP7-LT"
User Unlocked Session	This event is logged when a user unlocks his workstation	02-28-2014 08:52:07 Auth.Notice 192.168.34.31 Feb 27 22:52:16 : 2014/02/27 22:52:16 EST,1,545691,User Unlocked Session,0,4155,,,,,"User Man, Bat unlocked session 2 on host BRADSUPP7-LT"

Security event parsers



FortiNAC-OS Requirement: "syslog" option must be included in the "set allowaccess" command. See [Open ports](#) for details.

You can customize parsing of syslog messages for generating security events. When a syslog message is received from a device, the message is parsed using the format specified in the security event parser. You can also define severity level mappings between the vendor and FortiNAC.

In Topology, you will see enabled security event parsers listed as options when configuring a pingable device to parse incoming security events. See [Add or modify a pingable device on page 302](#).

To access security event parsers, select **System > Settings > System Communication > Security Event Parsers**.

Settings

Field	Definition
Table columns	
Name	The name of the security event parser.
Enabled	A green check mark indicates that the security event parser is enabled. A red circle indicates that the security event parser is disabled. When enabled, the security event parser is available in Topology. When disabled, the security event parser is not available.
Vendor	The name of the vendor of the device that generated the event.
Format	Message format for the security event parser. Supported formats include: CSV: Message is a series of data fields typically separated by commas. Comma separated value. Other characters can be used to separate data fields.

Field	Definition
	TAG/VALUE: Message is a series of fields each with a tag and a value. For example, the message could contain the following : cip=192.168.10.182. cip is the tag indicating that this is the IP address of the user causing the problem. 192.168.10.182 is the value associated with that tag. CEF: Message is a series of fields, some in a standard position, others with a tag and a value. For example the message could contain the following: src=192.168.10.182. src is the tag indicating that this is the IP address of the user causing the problem. 192.168.10.182 is the value associated with that tag.
CSV Delimiter	Character used to separate the fields in the security event parser. Most common options include: space, comma (,) and pipe (). This field is not available for the TAG/VALUE format.
Tag Delimiter	Character used to separate field name and value in the security event parser. This field is not available for the CSV format. A space is used as the delimiter.
Source/IP Column	The name of the field or number of the column containing the source IP address.
Destination IP Column	The IP address of the host or device the source host was communicating with.
Type Column	The type of security event received.
Subtype Column	The subtype of the security event.
Threat ID Column	A unique identifying code supplied by the vendor for the specific type of threat or event that occurred.
Description Column	A description supplied by the security appliance of the event.
Severity Column	Name of the field or number of the column containing the severity.
Right click options	
Modify	Modify the selected parser.
Delete	Deletes the selected parser.
Copy	Click to copy information from the selected parser to create a new security parser.
In Use	Shows which devices in Topology are currently using the parser.
Test	Allows you to test the security event parser by entering a syslog message received from a device.
Enable	Enables the parser.
Disable	Disables the parser.
Buttons	
Add	Add a parser.

Add or modify a security event parser

The security event parser allows you to customize parsing of syslog messages for generating security events.

1. Click **System > Settings**.
2. In Flat View, select **Security Event Parsers** from the tree.
3. Select the **Enabled** check box to enable the security event parser.
4. Enter a **Name** for the security event parser.
5. (Optional) To build the security parser using a received syslog message, click **Populate from Received Syslog**.
6. Use the table below to enter the file information.

Settings

Field	Definition
Populate from Received Syslog	Allows you to select a current syslog message to build the security event parser.  You must select the format of the selected syslog file from the Format drop-down list.
Enabled	Enables the security parser to be available as an option when configuring a pingable device to parse incoming security events
Name	Enter the name of the security event parser.
Vendor	Enter the name of the vendor of the device that will generated the event.
Format	Select the message format for the security event parser. Supported formats include: CSV: Message is a series of data fields typically separated by commas. Comma separated value. Other characters can be used to separate data fields. TAG/VALUE: Message is a series of fields each with a tag and a value. For example, the message could contain the following : cip=192.168.10.182. cip is the tag indicating that this is the IP address of the user causing the problem. 192.168.10.182 is the value associated with that tag. CEF: Message is a series of fields, some in a standard position, others with a tag and a value. For example the message could contain the following: src=192.168.10.182. src is the tag indicating that this is the IP address of the user causing the problem. 192.168.10.182 is the value associated with that tag.
Data fields	
Entire Column/Tag	When you select Entire Column/Tag in the Data Fields drop-down list, enter the name of the field or number of the column containing the value. The entire value will be used to create the security event.
Partial Column/Tag	When you select Partial Column/Tag in the Data Fields drop-down list, you can build a regular expression that lets you to define which parts of the column to use when creating the security event.  Refer to websites such as http://www.regular-expressions.info/ and https://www.debuggex.com/ for additional information about building regular expressions.

Field	Definition
Source/IP Column	Enter the name of the field or number of the column containing the source IP address. The entire value will be used to create the security event.
Destination IP Column	Enter the IP address of the host or device the source host was communicating with.
Type Column	Enter the type of security event received.
Subtype Column	Enter the subtype of the security event.
Threat ID Column	Enter the unique identifying code supplied by the vendor for the specific type of threat or event that occurred.
Description Column	Enter the description supplied by the security appliance of the event.
Severity Column	Enter the name of the field or number of the column containing the severity.
Severity mappings	
Source Value	The severity value provided by the vendor.
Severity Value	The severity value in FortiNAC to be mapped to the source value.
Add	Click to add a severity level mapping.
Add Range	Click to map a single severity value in FortiNAC to a range of values provided by the source.
Modify	Click to modify a severity mapping.
Delete	Click to delete a severity mapping.

Trap MIB files

The Trap MIB Files view allows you to enter a configuration to interpret SNMP trap MIB information sent from a device and associate it with events and alarms in FortiNAC.

Requirements

- FortiNAC-OS Requirement: "snmp" option must be included in the "set allowaccess" command. See [Open ports](#) for details.
- FortiNAC can only receive traps through SNMPv1 and SNMPv2 communications.
- To receive and interpret traps from devices or applications on your network, those devices or applications must be modeled in FortiNAC and have an associated IP address.
- The device or application must have traps configured to be sent to the IP address of the FortiNAC server.
- Map events to Alarms. When a trap is received, FortiNAC compares the trap to the information listed in the Trap MIB Files and searches for a match. If a match is found, an event is generated. If corresponding alarms have been mapped to the event, alarms are also triggered.
- Multiple traps can be added to a single Trap MIB.



It is recommended that you generate and capture a trap from the sending device to make sure that you are entering the correct information when configuring the Trap MIB files.

Settings



IP address OID, MAC address OID and user ID OID are not all required. Any one OID can be used to identify the host or user that triggered the trap.

Field	Definition
MIB File Name	Name of the MIB file. FortiNAC creates the file when the Custom Trap data is entered. Any MIB file can have multiple custom traps.
Trap OID	The Trap OID compiled by FortiNAC based on the data entered in the Custom Trap section. More than one Custom Trap can be associated with a single Trap MIB file.
Label	Label used to identify the trap in the event and alarm configuration.
Specific Type	This a number that is specific to the sending device. For example, if you are looking for a trap from a Cisco device, you would enter a number that corresponds to Cisco specific traps.
Enterprise OID	OID associated with the enterprise or manufacturer of the device sending the trap. For example, if FortiNAC were watching for traps from a Cisco device the enterprise OID would be 1.3.6.1.4.1.9.
IP address OID	OID associated with the trap varbinds that contain the IP address of the host that is triggering the trap.
MAC address OID	OID associated with the trap varbinds that contain the Physical Address of the host that is triggering the trap.
User ID OID	OID associated with the trap varbinds that contain the user ID of the user logged onto the host that is triggering the trap.
Alarm Cause	Textual description of the probable cause of the alarm.
Event Format (Java Message API)	Textual description of the event which includes a variable for the varbind information to be displayed from the trap. For example, if you have entered "Event caused by {4}." Whatever data is contained in the fifth varbind in the trap, is included in the message. The number 4 represents the fifth varbind because the count begins with 0.
Buttons	
Add MIB	Opens the Add MIB dialog and allows you to add both the MIB and the associated custom trap.
Add Custom Trap	Select a MIB in the Trap MIBs list and use this option to add another custom trap to the MIB. Opens the Add MIB dialog with the name of the selected MIB completed and blank custom trap fields.
Modify	If the MIB is selected, allows you to modify the name. If the custom trap is selected, allows you to modify the trap information.

Configure MIB files and custom traps

1. Click **System > Settings**.
2. Expand the **System Communication** folder.
3. Select **Trap MIB Files** from the tree.
4. Click **Add MIB** or select a MIB and click **Add Custom Trap**.
5. Enter the **trap information** using the settings shown in the table.
6. Click **OK** to save.

System management

System Management groups together core server features such as data backup and restore, redundant servers, licensing and time zone settings. Options include:

Option	Definition
Database Archive	Set the age time for archived data files and configure the schedule for the Archive and Purge task. See Database archive on page 977 .
Database Backup/Restore	Schedule database backups, configure how many days to store local backups, and restore a database backup. Note that this restores backups on the FortiNAC server, not backups on a remote server. See Database backup/restore on page 980 .
High Availability	Configuration for primary and secondary appliances for high availability. Saving changes to these settings restarts both the primary and secondary servers. See High availability on page 981 .
License Management	View or modify the license key for this server or an associated Application server. See License management on page 983 .
NTP and Time Zone	Reset the time zone and NTP server for your FortiNAC appliances. Typically the time zone and NTP server are configured using the Configuration Wizard during the initial appliance set up. Requires a server restart to take effect. See NTP and time zone on page 985 .
Power Management	Reboot or power off the FortiNAC server. See Power management on page 986 .
Remote Backup Configuration	Configure Scheduled Backups to use a remote server via FTP and/or SSH. See Remote backup configuration on page 986 .
System Backups	Create a backup of all system files that are used to configure FortiNAC. See System backups on page 990 .

Custom Health Check

Overview

In server load balancing deployments, the system uses health checks to poll the members of the real server pool to test whether an application is available. The user can also configure additional health checks to poll related servers, and include results for both in the health check rule. For example, the user can configure a TCP health check test and an ICMP health check test as well.

This feature assesses the health of a CA using certain health check types (i.e. protocols) like ICMP, TCP, and TCP Echo.

Custom Health Check (for Leader, Cluster off FortiNAC-M, CA 7.6) is an optional feature that users can use in addition to the Predefined Health Check. Predefined and Custom Health Check, if enabled, will determine the Status of the CA, which will be reflected in **CA Management > Status**.

Predefined Health Check Types

ICMP – Pings the server

TCP Echo (F 7.6.0 - F 7.6.2 only) - Sends a TCP echo to server port 7. Expects the server to respond with the corresponding TCP echo.

TCP – Specify port (listening port number of the backend server) as an input.

RADIUS (F 7.6.0 - F 7.6.2 only) – Listening port number of the backend server. Default RADIUS is **1812**.

- Port
- Username
- Password
- Password Type: User or CHAP
- Secret Key
- Radius Reject : Enable or Disable

To create a custom health check rule:

1. Go to **Settings > Custom Health Check > Create New +**.
2. Create your health check rule with the fields below.

Setting	Description
Name	Configuration name
Type	
ICMP	Simple ping to test connectivity.
TCP Echo (F 7.6.0 - F 7.6.2 only)	Simple ping to test connectivity.
RADIUS (F 7.6.0 - F 7.6.2 only)	User needs to specify the port (listening port number of the backend server).

Setting	Description
	Port — Listening port number of the backend server. Username — Specify username Password — Specify password Password Type - User Secret Key — Secret key to be used in RADIUS server. - CHAP RADIUS Reject Enable/disable the RADIUS server in FortiNAC.
TCP	User needs to specify the port (listening port number of the backend server)
Retry	Attempts to retry the health check to see if a down server has become available. The default is 1 . 1. Make sure the input is within required range. 2. Tooltip: Enter a retry number between 0 and 10.
Timeout	Seconds to wait for a reply before assuming that the health check has failed. The default is 3 1. Make sure input is within required range. 2. Tooltip: Enter a timeoutnumber between 1 and 60.



Custom health check when CA is managed by FortiNAC Manager

When the CA is managed by FortiNAC Manager, the following is changed for Custom Health Check:

- The user can no longer configure and change Custom Health Check in CA. The changes must happen in FortiNAC-M.
- All add, edit or delete operations are disabled in CA.
- Existing Custom Health Check and Custom Health Check rules will be synced to the FortiNAC-M.

Database archive

Use database archive to set age times for selected log files. Log files are archived and then purged from the FortiNAC database when the age time elapses. Archived data can be imported back into the database if necessary. Importing archived data does not overwrite existing data it adds the archived records back into the database. See [Import archived data on page 102](#).

Settings

Field	Definition
Remove local backups older than	Number of days for which you would like to keep backups. Anything older than the number of days entered, is removed the next time the scheduled task for backups runs. This setting removes backup files created on the FortiNAC server before they are copied to the remote server. Backups on the remote server are not removed.  The timing of the scheduled backup task and the age of the files that are to be removed must be thought out carefully or you will remove all of your backups. For example, if the remove option is set to 5 days and your backup task runs every 15 days, you may inadvertently remove all of your backups. However, if the remove option is set to 15 days and the backup task runs every 5 days, then you would always have backup files.
Event/Alarms Age Time (days)	Number of days events or alarms are maintained in the Events or Alarms logs and viewable in the Events or Alarms View. Events and Alarms are archived and purged based on the scheduled task settings. Default setting = 7 days
Scan Results Age Time (days)	Number of days Scan results are maintained in the Scan results log and viewable in the Scan results view. Scan results are archived and purged based on the scheduled task settings. Default setting = 7 days

Edit archive age time

1. Click **System > Settings**.
2. Expand the **System Management** folder.
3. Select **Database Archive** from the tree.
4. Use the information in the table above to set **Age Time**.
5. Click **Save Settings**.

Schedule event archive and purge

1. Click **System > Settings**.
2. Expand the **System Management** folder.
3. Select **Database Archive** from the tree.
4. Click **Modify Schedule**.
5. Select the **Enabled** check box.
6. Enter a name for the task in the **Name** field.
7. The **Description** field is optional. Enter a description of the task.
8. Action type and Action are pre-configured based on the task and cannot be modified.
9. From the **Schedule Type** drop down list, select either **Fixed Day** or **Repetitive** and set the day and time that the task is to be performed.

10. A **Fixed Day Task** is one in which you schedule a task to run on a combination of days of the week and times of the day, such as Mondays at 1:00 pm and Fridays at 10:00 am. Select the day(s) and time to run the task.
- Click the **box** next to the day(s) to select the day.
 - Click the **down arrows** and select the hour, minutes, and AM or PM from the drop-down list for each day.
 - To enter days/times more quickly, select **Set Multiple Days** to set multiple days with the same time.
 - To remove all settings, click **Clear All**.
11. A **Repetitive Task** is one that you schedule to start on a given day, at a certain time, for the number of times you specify, such as every 10 days starting today. The repetition rate can be set to any number of minutes, hours, or days.
- Enter the **Repetition Rate** using whole numbers.



A repetition rate of zero causes the task to run only once.

- Click the **down arrow** and select Minutes, Hours, or Days from the drop-down list.
- Enter the **date and time** for the task to run in the **Next Scheduled Time** field using the format MM/DD/YY hh:mm AM/PM Time Zone.



The new Repetition Rate does not take effect immediately. It starts the next time the scheduled task runs. For the new Repetition Rate take effect immediately, click **Update**.

- Click **Update** to update the **Next Scheduled Time** field or change the **Repetition Rate**.

12. Click **OK**.

Schedule settings

Field	Definition
Remove local backups older than	Number of days for which you would like to keep backups. Anything older than the number of days entered, is removed the next time the scheduled task for backups runs. This setting removes backup files created on the FortiNAC server before they are copied to the remote server. Backups on the remote server are not removed. The timing of the scheduled backup task and the age of the files that are to be removed must be thought out carefully or you will remove all of your backups. For example, if the remove option is set to 5 days and your backup task runs every 15 days, you may inadvertently remove all of your backups. However, if the remove option is set to 15 days and the backup task runs every 5 days, then you would always have backup files.
Status	Indicates whether the task is enabled or disabled.
Schedule Interval	How often the scheduled task runs.
Next Scheduled Time	The next date and time the scheduled synchronization task will run. Entered in the format MM/DD/YY HH:MM AM/PM
Modify Schedule	Allows you to modify the scheduled activity.
Run Now	Runs the scheduled task immediately.

Database backup/restore

A database backup creates a backup of the entire database. All database archives can be restored if the database becomes corrupted. To restrict the restoration to only alarms, connections, or events data, go to those specific views and select the Import option. See [Alarms on page 783](#), [Connections view on page 1](#), and [Events on page 749](#) for more information.

Restoring a database archive causes the FortiNAC Server to restart.

1. Click **System > Settings**.
2. Expand the **System Management** folder.
3. Select **Database Backup/Restore** from the tree.

Schedule a database backup

1. Under **Schedule Database Backup**, click **Modify Schedule**.
2. Select the **Enabled** check box.
3. Enter a name for the task in the **Name** field.
4. The **Description** field is optional. Enter a description of the task.
5. Action type and Action are pre-configured based on the task and cannot be modified.
6. From the **Schedule Type** drop down list, select either **Fixed Day** or **Repetitive** and set the day and time that the task is to be performed.
7. A **Fixed Day Task** is one in which you schedule a task to run on a combination of days of the week and times of the day, such as Mondays at 1:00 pm and Fridays at 10:00 am. Select the day(s) and time to run the task.
 - a. Click the **box** next to the day(s) to select the day.
 - b. Click the **down arrows** and select the hour, minutes, and AM or PM from the drop-down list for each day.
 - c. To enter days/times more quickly, select **Set Multiple Days** to set multiple days with the same time.
 - d. To remove all settings, click **Clear All**.
8. A **Repetitive Task** is one that you schedule to start on a given day, at a certain time, for the number of times you specify, such as every 10 days starting today. The repetition rate can be set to any number of minutes, hours, or days.
 - a. Enter the **Repetition Rate** using whole numbers. A repetition rate of zero causes the task to run only once.
 - b. Click the **down arrow** and select Minutes, Hours, or Days from the drop-down list.
 - c. Enter the **date and time** for the task to run in the **Next Scheduled Time** field using the format MM/DD/YY hh:mm AM/PM Time Zone.
 - d. Click **Update** to update the **Next Scheduled Time** field or change the **Repetition Rate**.

The new Repetition Rate does not take effect immediately. It starts the next time the scheduled task runs. For the new Repetition Rate take effect immediately, click **Update**.
9. Click **OK**.

Schedule settings

Field	Definition
Remove local backups older than	Number of days for which you would like to keep backups. Anything older than the number of days entered, is removed the next time the scheduled task for backups runs. This setting removes backup files created on the FortiNAC server before they are copied to the remote server. Backups on the remote server are not removed. The timing of the scheduled backup task and the age of the files that are to be removed must be thought out carefully or you will remove all of your backups. For example, if the remove option is set to 5 days and your backup task runs every 15 days, you may inadvertently remove all of your backups. However, if the remove option is set to 15 days and the backup task runs every 5 days, then you would always have backup files.
Status	Indicates whether the task is enabled or disabled.
Schedule Interval	How often the scheduled task runs.
Next Scheduled Time	The next date and time the scheduled synchronization task will run. Entered in the format MM/DD/YY HH:MM AM/PM
Modify Schedule	Allows you to modify the scheduled activity.
Run Now	Runs the scheduled task immediately.

Restore a database

1. Click on a backup to select it.
2. Click **Restore Database**.

High availability

Use the high availability view in the FortiNAC GUI to add to and update high availability configuration information. See **Configure high availability** below.

For details on *required* prerequisites prior to configuring High Availability, refer to the High Availability reference manual in the Document Library.

[High Availability - FortiNACOS](#)

Configure high availability

1. Ensure that all appliances are keyed for high availability. See [License management on page 983](#) and check the high availability field.
2. Click **System > Settings**.
3. Expand the **System Management** folder.
4. Select **High Availability** from the tree.
5. Use the table below to enter the required information.
6. Click **Save Settings** and wait for the success message.
7. Restart FortiNAC services on both appliances to apply changes. See [Power management](#).



When you click **Save Settings** on the **Administration - High Availability** view, the primary server tries to communicate with the secondary to ensure that the database will be replicated. If the primary server cannot communicate with the secondary, it continues to try until communication is established.



Note: For steps to remove an existing High Availability configuration, refer to the Appendix of the High Availability reference manual in the Fortinet Document Library.

<https://docs.fortinet.com/document/fortinac-f/7.6.0/high-availability-fortinac-os/626202/remove-high-availability-configuration>

Settings

Field	Description
Shared IP configuration	
Use Shared IP address	Enables the use of a shared IP address in the high availability configuration. If enabled, the administrator can manage whichever appliance that is in control with the shared IP address instead of the actual host IP address. If your primary and secondary servers are not in the same subnet, do not use a shared IP address.
Shared IP address	The shared IP address for the high availability configuration. Added to the <code>/etc/hosts</code> file when the configuration is saved.
Shared Subnet Mask (bits)	The shared subnet mask in dotted decimal (example: 255.255.255.0).
Shared Host Name	Part of the entry in the <code>/etc/hosts</code> file for the shared IP address. Administrators can access the UI using either the shared IP address or the shared host name.
Server configuration	
Primary Appliance	IP address: IP address assigned to port1 for the primary. Gateway IP address: IP address pinged by the appliances to determine if network connectivity is still available. CLI/SSH root Password [User:root]: Root password on the appliance itself. Allows settings to be written to the appliance. Retype root CLI/SSH Password [User:root]: Retype the password entered in the CLI/SSH root Password field for confirmation.
Secondary Appliance	IP address: IP address assigned to port1 for the secondary. Host Name: Name assigned to the secondary. Gateway IP address: IP address that is pinged by the appliances to determine if network connectivity is still available. CLI/SSH root Password [User:root]: Root password on the appliance itself. Allows settings to be written to the appliance. Retype root CLI/SSH Password [User:root]: Retype the password entered in the CLI/SSH root Password field for confirmation.

Use of Port 3 for Out-of-Band MGMT



This feature only applies to FortiNAC Manager version 7.6.2 and above.

Port 3 can be used as Out-of-Band MGMT Interface when configuring High Availability for both Primary and Secondary appliances. To take advantage of Port 3, both Primary and Secondary Appliances will need to be added manually.

For example:

1. On CA primary and secondary appliances CLI, configure ip through port3:

```
configure system interface
  edit port3
    set ip <Primary or Secondary Appliance IP address>
    set allowaccess http https https-adminui ssh
    config ipv6
  end
next
end
```

2. On FortiNAC Control Manager, go to **System > CA Management**, and add both port 3 IP addresses from step 1. Then the Primary and Secondary Appliances will recognize each others as a pair for High Availability.

License management

Manage license keys on the servers through this view. Servers that are part of a high availability configuration appear in the drop-down list.

License information is displayed on the dashboard. See [Dashboard on page 86](#) for additional information.

License information can also be displayed through FortiNAC CLI. See [Show License Information](#) for more details.

The events related to license use help maintain proper appliance use per environment. Warning and critical events and alarms are generated based on a set of user defined thresholds.

See [Event thresholds on page 774](#) to set thresholds. See [Map events to alarms on page 784](#) to set alarms based on threshold events.

Installing a new license key with a different serial number

Important: Installing a new license key with a different serial number than the existing key on FortiNAC Manager VM's is currently not supported. Most commonly seen in environments where a license has expired and a new license must be registered and installed. This causes unexpected behavior in FortiNAC manager. Therefore, the Manager must be factory reset and reconfigured after the new license key has been installed.

See article for details:

[New license key with different serial number on Manager causes unexpected behavior](#)

View/modify license information

The license options will vary depending on whether pre-2016 (Secure Enterprise Standard, Secure Enterprise Advanced, or Secure Enterprise Mobility) or post-2016 (Secure Enterprise Advanced or Secure Enterprise Premier) license packages are installed on the server.

1. Click **System > Settings**.
2. Expand the **System Management** folder.
3. Select **License Management** from the tree.
4. From the drop-down list select the server containing the license key.
5. Click **Modify License Key**.
6. You can modify the license key in two ways:
 - To upload from a text file, click **Upload**, browse to the license key file, and click **Open**. This must be a text file not a zip file.
 - From another file, copy and paste the new license key text into the text box.
7. Click **OK** to apply the new license key. The existing key detail is displayed in a pop-up window along with the new key detail.
8. Click **OK** to apply the new license key. Click **Undo** if you want to revert to the existing license key.
9. **To restart the server immediately**, click **OK** on the dialog box.
10. **To restart the server later**, click **Cancel** on the dialog box. Another dialog box appears stating that the new key will not be applied until the server is restarted. New features or license counts contained in the new license cannot be accessed until the server is restarted. The new license is saved on the server, but is not read until the server is restarted.
11. Click **OK** to confirm.

Settings

Key	Definition
License Name	Indicates which license level (Base, Plus or Pro) is installed on the server. Note: Subscription license entitlements display for the Secondary Server when it is "Running - in Control" in a High Availability pair.
Concurrent Licenses	Number of licenses configured for possible online connections to the network. Connections are counted for hosts and devices that are not switches or routers. Note: Subscription license entitlements display for the Secondary Server when it is "Running - in Control" in a High Availability pair.
Security Incidents Licenses	Indicates the number of licenses configured for Security Incidents.
Evaluation Time	Indicates the number of days configured for an evaluation license. If you have purchased a full license for the product, this field does not display.
High Availability	Indicates whether or not high availability has been enabled.
Device Profiler	Indicates whether or not the device profiler feature has been enabled.
Guest Manager	Indicates whether or not the guest manager feature has been enabled.
Endpoint Compliance	Indicates whether or not the Security Policy features have been enabled.

Key	Definition
Integration Suite	Indicates whether or not access to third party information such as SNMP Traps and Syslogs has been enabled.
Wireless Only	Indicates whether or not a limited Wireless Only license has been enabled. Provided as a quick start solution for organizations that use only wireless devices on their network. This feature is not supported for all wireless devices. Currently only HP MSM and Ruckus controllers can be configured. For HP wireless devices, FortiNAC can write configuration changes to the device. For Ruckus controllers, FortiNAC cannot write configuration changes to the device only the device model in the database. Other wireless devices and up to five wired devices can be added using the Network Devices View or the Inventory. In addition, this license disables the Discovery feature. .

NTP and time zone

You can reset the time zone and NTP server for your FortiNAC appliances. Typically the time zone and NTP server are configured using the configuration wizard during the initial appliance set up.

The NTP server is used to synchronize the clock on the FortiNAC appliance. FortiNAC contacts the NTP server periodically to synchronize its clock with the NTP servers. NTP server keeps time in UTC, or Coordinated Universal Time, which corresponds roughly to Greenwich Mean time.

Settings

Field	Definition
FortiNAC Servers	Provides a list of servers for which you can change time settings. Each server's time must be set individually. Settings apply only to the server displayed in this field.
NTP Server	External server used to synchronize or update the clock on the selected FortiNAC server. Defaults to pool.ntp.org.
Time Zone	Time zone where the selected FortiNAC server resides.

Modify time settings



Changes to NTP or time zone require a server restart to take effect. Go to the control panel to restart the server now. See [Power management on page 986](#).

1. Click **System > Settings**.
2. Expand the **System Management** folder.
3. Select **NTP And Time Zone** from the tree.
4. Click the **FortiNAC Servers** drop-down and choose the server to be modified.
5. Enter your preferred NTP Server in the **NTP Server** field.
6. Click the **Time Zone** drop-down and select the time zone for this server.

7. Click **Save Settings** to save settings for the selected server.
8. To modify another server, select it in the FortiNAC Servers drop-down and repeat steps 4 through 7.

Power management

The system can be rebooted or powered down through the FortiNAC interface, by any user whose administrator profile allows access to the Settings view. In a high availability environment, servers must be rebooted or powered off individually.



In a HA environment, reboot or power off the secondary servers first.

Events associated with Power Management are as follows:

- **System Power Off:** Indicates that the server has been powered down and provides the user name of the user who initiated the action.
- **System Reboot:** Indicates that the system was rebooted and provides the user name of the user who initiated the action.

Reboot the server

1. Click **System > Settings**.
2. Expand the **System Management** folder.
3. Select **Power Management** from the tree.
4. Select a server from the list.
5. Click **Reboot**. This process may take 2-3 minutes.

Power off the server

1. Click **System > Settings**.
2. Expand the **System Management** folder.
3. Select **Power Management** from the tree.
4. Select a server from the list.
5. Click **Power Off**. This process may take 30 seconds.

Remote backup configuration

Use the Remote Backup Configuration view to define the connection details used to copy database and system files to a third party (remote) server.

Database and system backups occur automatically when the Database BackUp and System Backup scheduled tasks run. The backup files are stored on the local appliance. See

Database backup/restore and System backups for more information.

The Administrator can, additionally, configure FortiNAC to place a copy of the database and system backups on a remote server for safekeeping. The backups are placed in time and date stamped files.

Files can be transferred using FTP and/or SSH protocols.

Database backup file naming convention:

FortiNAC_DataBase_BackUp_YYYY_MM_DD_HH_mm_SS_<hostname>.gz

System backup file naming convention:

<hostname>.YYYYMMDD.*.gz

Archive backup file naming convention:

MAC_RESULTS_Archive_YYYY_MM_DD_HH_mm_SS_localhost.bua.gz

RESULTS_Archive_YYYY_MM_DD_HH_mm_SS_localhost.bua.gz

TESTS_RESULTS_Archive_YYYY_MM_DD_HH_mm_SS_localhost.bua.gz

1. In the FortiNAC UI, navigate to **System > Settings > System Management > Remote backup configuration**.
2. Configure using the table below.

Field	Definition
Backup Timeout	Number of minutes for the backup to be created and copied to the remote server. If this time elapses before the backup is done, the process is interrupted. Be sure to select a time that is long enough for your system to complete its backup. The default is 20 minutes; however, large systems may require more time.
Number of days for local backups	The number of days to keep local backup files.
Number of days for local database backups	The number of days to keep local full database backup files.
Number of days for local archive backups	The number of days to keep local full database archive files.

Configure the applicable remote server option below.

Remote server configuration using FTP

1. Create an account on the remote FTP server to be used by FortiNAC for backup file transfer.
2. Create a folder to which FortiNAC will copy the files.
3. For instructions on completing the above tasks, consult documentation specific to the FTP application used.
4. Select the checkbox next to **EnableFTP Remote Backup**.

5. Configure using the table below.

Field	Definition
Server	IP address of the remote server.
User Name	User Name required for write access to the server.
Password	Password required for write access to the server.
Remote Path	The directory path where the remote backup files will be placed. This directory must exist on the server.

6. Save Settings.

Validate

1. Navigate to **System > Scheduler**.
2. Highlight the **Database Backup** task and click **Run Now**.
3. Highlight the **System Backup** task and click **Run Now**.
4. Highlight the **Database Archive and Purge** task and click **Run Now**.

On the remote server, confirm the files were transferred.

Remote server configuration using SSH

The FortiNAC's public key must be appended to the authorized_keys file in the remote server for successful SSH communication.

High Availability configurations: SSH keys for both the primary and secondary FortiNAC servers must be appended.

1. Select the checkbox next to **Enable SSH Remote Backup**.
2. Configure using the table below.

Field	Definition
Server	IP address of the remote server.
Remote Path	The directory path where the remote backup files will be placed. This directory must exist on the server.

3. **Save Settings**.
4. Select **Display Public SSH Keys**.
5. The Public SSH Key window appears. Copy the key displayed.
6. Click **Close**.
7. Associate the public key to the remote server where the backups will be stored. This process will vary depending on the product. Refer to the SSH server product documentation for instructions.



- The format of authorized_keys file is one entry per line.
- Do not include extra white space or characters when pasting the key.

Validate

1. Click **Test SSH Connection** to verify SSH communication with the remote server.
2. Once successfully tested, navigate to **System > Scheduler**.
3. Highlight the **Database Backup** task and click **Run Now**.
4. Highlight the **System Backup** task and click **Run Now**.
5. Highlight the **Database Archive and Purge** task and click **Run Now**.
6. On the remote server, confirm the files were transferred.

Remote server configuration using Secure FTP Remote Backup (SFTP)

1. Select the checkbox next to **Enable Secure FTP Remote Backup**.
2. Configure using the table below.

Field	Definition
Server	IP address of the remote server.
Remote Path	The directory path where the remote backup files will be placed. This directory must exist on the server.

3. **Save Settings.**
4. Select **Display Public SSH Keys**.
5. The Public SSH Key window appears. Copy the key
6. Click **Close**.
7. Associate the public key to the remote server where the backups will be stored. This process will vary depending on the product. Refer to the SSH server product documentation for instructions.



The format of authorized_keys file is one entry per line.
Do not include extra white space or characters when pasting the key.

Validate

1. Click Test SFTP Connection to verify communication with the remote server.
2. Once successfully tested, navigate to **System > Scheduler**.
3. Highlight the **Database Backup** task and click **Run Now**.
4. Highlight the **System Backup** task and click **Run Now**.
5. Highlight the **Database Archive and Purge** task and click **Run Now**.
6. On the remote server, confirm the files were transferred.

System backups

A system backup creates a backup of all system files that are used to configure FortiNAC, such as license key and web server configurations.

1. Click **System > Settings**.
2. Expand the **System Management** folder.
3. Select **System Backups** from the tree.
4. In the **Remove local backups older than field**, enter the number of days for which you would like to keep backups.

The timing of the scheduled backup task and the age of the files that are to be removed must be thought out carefully or you will remove all of your backups. For example, if the remove option is set to 5 days and your backup task runs every 15 days, you may inadvertently remove all of your backups. However, if the remove option is set to 15 days and the backup task runs every 5 days, then you would always have backup files.
5. Click **Modify Schedule**.
6. Select the **Enabled** check box.
7. Enter a name for the task in the **Name** field.
8. The **Description** field is optional. Enter a description of the task.
9. **Action type** and **Action** are pre-configured based on the task and cannot be modified.
10. From the **Schedule Type** drop down list, select either **Fixed Day** or **Repetitive** and set the day and time that the task is to be performed.
11. A **Fixed Day Task** is one in which you schedule a task to run on a combination of days of the week and times of the day, such as Mondays at 1:00 pm and Fridays at 10:00 am. Select the day(s) and time to run the task.
 - a. Click the **box** next to the day(s) to select the day.
 - b. Click the **down arrows** and select the hour, minutes, and AM or PM from the drop-down list for each day.
 - c. To enter days/times more quickly, select **Set Multiple Days** to set multiple days with the same time.
 - d. To remove all settings, click **Clear All**.
12. A **Repetitive Task** is one that you schedule to start on a given day, at a certain time, for the number of times you specify, such as every 10 days starting today. The repetition rate can be set to any number of minutes, hours, or days.
 - a. Enter the **Repetition Rate** using whole numbers. A repetition rate of zero causes the task to run only once.
 - b. Click the **down arrow** and select **Minutes**, **Hours**, or **Days** from the drop-down list.
 - c. Enter the **date and time** for the task to run in the **Next Scheduled Time** field using the format MM/DD/YY hh:mm AM/PM Time Zone.
 - d. Click **Update** to update the **Next Scheduled Time** field or change the **Repetition Rate**.

The new repetition rate does not take effect immediately. It starts the next time the scheduled task runs. For the new repetition rate take effect immediately, click **Update**.
13. Click **OK**.
14. Click **Save Settings**.

Settings

Field	Definition
Remove local backups older than	Number of days for which you would like to keep backups. Anything older than the number of days entered, is removed the next time the scheduled task for backups runs. This setting removes backup files created on the FortiNAC server before they are copied to the remote server. Backups on the remote server are not removed. The timing of the scheduled backup task and the age of the files that are to be removed must be thought out carefully or you will remove all of your backups. For example, if the remove option is set to 5 days and your backup task runs every 15 days, you may inadvertently remove all of your backups. However, if the remove option is set to 15 days and the backup task runs every 5 days, then you would always have backup files.
Status	Indicates whether the task is Enabled or Disabled.
Schedule Interval	How often the scheduled task runs. Options are Minutes, Hours, or Days.
Next Scheduled Time	The next date and time the scheduled synchronization task will run. Entered in the format MM/DD/YY HH:MM AM/PM
Modify Schedule	Allows you to modify the scheduled activity.

Updates

Updates groups together options for updating FortiNAC servers with the latest software release and the latest Agent packages.

Options

Option	Definition
Agent Packages	Agent Update Settings: Agent Update can be configured here on connection settings for the download location. See Agent updates on page 1001 for more details. Agent Packages: Displays a list of the Dissolvable Agent, Persistent Agent, and Passive Agent versions available on your FortiNAC appliance. Download new agents and add them to FortiNAC as they become available from Fortinet using the Download. Download an Administrative template for GPO configuration to your PC from the FortiNACappliance using the links at the top of the view. See Agent packages on page 992.
System	System installation is available at system, provided by FortiGuard Distribution Network. The latest system updates is automatically synchronized through FortiGuard. See System System version information can be viewed in the System Summary Widget in the Dashboard of the UI.

Option	Definition
	Example Version 7.2.1.0051

Agent packages

The Agent packages view displays a list of the Dissolvable Agent, Persistent Agent, Passive Agent, and Mobile Agent versions available on your FortiNAC appliance. This view allows you to download new agents and add them to FortiNAC as they become available from Fortinet.

Both the Dissolvable Agent and Persistent Agents can be supplied to hosts automatically by FortiNAC through the captive portal when the host reaches the appropriate web page. The agent presented to the host is based on the configuration of the endpoint compliance policy applied to that host. Supplying the Passive Agent requires additional configuration. See [Passive Agent on page 604](#).

Hosts who already have a version of the Persistent Agent installed can be automatically updated to a newer version of the agent based on the settings you enter on the Agent Update tab. See [Upgrade the Persistent Agent on page 504](#).

You also have the option to download a Persistent Agent from the list to your own computer to be distributed to hosts through your web site, using a login script or some other distribution method. Files are saved on your computer in the default download location. This location varies depending on the browser you are using.

The Windows Persistent Agent is available in two formats: .msi and .exe. The .msi file is recommended for use in a managed install by non-user-interactive means. The .exe file is recommended for user-interactive installation. The Linux Persistent Agent is also available in two formats: .deb or .rpm. The macOS Persistent Agent is available in .dmg format.

If you choose to distribute the agent using Group Policy Objects, you must download and install administrative templates on your Windows server. Click **Download Administrative Agent Template** to download the templates.

Select an agent and click **Delete** to remove old Agent packages from your server.

Settings

Field	Definition
Package Name	Name of the .jar file containing the agents and supporting files.
Version	Version number of the agent.
Name	Name of the type of agent. Agents include: • Mobile Agent • Dissolvable Agent • Persistent Agent • Passive Agent
Operating System	Operating system on which the agent can run.
File Name	File name and type, such as .exe or .bin.
Size	Download size of the agent file in KiB.
Delete	Allows you to delete old agent packages from the FortiNAC server.

Field	Definition
Download agent packages	
Status	Indicates whether there are new agent packages available for download from Fortinet. Status messages include: - Up to Date - New Agent Packages Available
Name	Name of the agent package to be downloaded

Download new agent packages

New Agent packages are placed on the Fortinet update server when they become available. Agent packages contain all of the available FortiNAC agents and agent related files. The Mobile Agent can be downloaded from the captive portal if the device allows downloads from unknown sources, otherwise it is distributed through Google Play. However, there are supporting files for the Mobile Agent in the agent package. For any agent update you must download and install the latest agent package.

Note: Agent F 7.6.0 introduced a new naming convention for the agent package .jar file (FNACAgent-v7.6.x.xxxx.jar). The agent package filenames displayed will depend upon the FortiNAC version.

FortiNAC F 7.6.0, F 7.4.0, F 7.2.8 and lower: Only the older filename (agent*) is displayed.

FortiNAC F 7.6.1, F 7.4.1, F 7.2.9 and greater: Both filenames are displayed.

The FortiNAC versions that display both filename conventions for the same agent package can work with either one. For additional details, see [Agent Release Notes](#).

Download settings must be configured correctly in order to download agent packages. See [Agent updates on page 1001](#) for more information.

1. Click **System > Settings**.
2. Expand the **Updates** folder.
3. Select **Agent Packages** from the tree.
4. Scroll to the bottom of the page. When new agents are available, the message **New Agent Packages Available** is displayed next to **Download**. Select **Download** to display a list of available agent packages.
5. Click the **Download** link next to an agent package to initiate the download. A progress page is displayed until the download is complete.
6. Click **Close** to return to the **Agent Packages** view.

Download the Persistent Agent for custom distribution

Follow the steps below to download a Persistent Agent from your FortiNAC appliance to your local computer.

1. Click **System > Settings**.
2. Expand the **Updates** folder.
3. Select **Agent Packages > Agent Packages** from the tree.



The Dissolvable Agent, Persistent Agent, and Passive Agent packages are included in the list, but only the Persistent Agent and Passive Agent packages may be downloaded through this view. The links appear in blue.

4. Locate the agent you wish to download, select and click **Download Agents**.
5. The file is typically saved to the default download location. This is controlled by your browser.
6. Distribute the file via the Desktop Management software of your choice. It is recommended that you visit our web site for additional information on deploying the Persistent Agent outside of FortiNAC.

Download and configure administrative templates for GPO

Administrative templates are used to configure registry settings on **Windows** endpoints through Group policy objects. For the Persistent Agent and the Passive Agent, there are templates to configure the Server URL of the FortiNAC Application Server with which the agent will communicate. There are also per-computer and per-user templates to enable or disable the system tray icon or Balloon Notifications of status changes. The Balloon Notification template does not affect the Server IP and is not required.

FortiNAC does not support an Administrative Template for deploying configuration changes to macOS computers or users through GPO. You can investigate 3rd party applications, such as Likewise Enterprise that support macOS computers using Group Policy Object editor. The modifications shown in the tables below can be made in the Preferences file on macOS hosts, using the tool of your choice.



The Persistent Agent running on a macOS computer can determine the server to which it should connect via DNS server records it does not require changes to Preferences.

If you are using the Persistent Agent, your Windows login credentials are automatically passed to FortiNAC. You can modify the Administrative Template to hide the Persistent Agent Login dialog and use the Windows login credentials sent by the Persistent Agent by modifying the settings in the Administrative Template. See [Using Windows domain login credentials on page 502](#).

Security is enabled by default. It is recommended that you update to the latest template files and configure the templates for the new security settings.

Requirements:

- Active Directory
- Group Policy Objects
- Template Files From Fortinet

Templates:

The templates listed below are provided by Fortinet. You must run the installation program for the templates on your Windows server. Be sure to select the appropriate MSI for your Windows server architecture.

- 32-bit (x86): Bradford Networks Administrative Templates.msi
- 64-bit (x86_64): Bradford Networks Administrative Templates-x64.msi

Install the templates for GPO

1. In FortiNAC select **System > Settings > Updates > Agent Packages**.
2. At the top of the Agent Distribution window click either the **32-bit (x86)** or the **64-bit (x86_64)** link to download the appropriate template file.
3. Copy the template file to the domain server.

4. On the domain server, double-click the msi file to start the installation wizard.
5. Click through the installation wizard. When installation has completed, the Microsoft Group Policy Management Console is required to complete the installation. Refer to the Windows Server documentation for details.
6. Navigate to the **Group Policy Object** you want to edit, right-click and select **Edit** to display the GPO Editor pane.
7. Right-click **Computer Configuration > Administrative Templates** and select **Add/Remove Templates**, shows the current templates pop-up.
8. Click **Add** and browse to **Program Files\Bradford Networks\Administrative Templates**.
 - a. To use the Persistent Agent, select `FortiNAC Persistent Agent.adm` and click **Open**.
 - b. To use the Passive Agent, select `FortiNAC Passive Agent.adm` and click **Open**.
9. Click **Close**, and the Administrative Templates will be imported into the GPO.

Install an updated template when balloon notifications are configured

If you have never configured Balloon Notifications, go to the section of this document labeled Install An Updated Template.

If you already have a Fortinet Administrative Template installed for the Persistent Agent and the Balloon Notifications were ever set to anything other than Not Configured (e.g. enabled or disabled), you must unconfigure the Balloon Notifications and push the settings to your clients. When your clients have all been updated, then the new template can be installed. These templates affect the registry settings on the client host. In the case of the Balloon Notifications, removing the previous configuration before installing the new one ensures that the keys will be set correctly.



Before updating a template, be sure to record the current template settings. Existing template settings are lost when the new template is installed.

1. In FortiNAC, navigate to **System > Settings > Persistent Agent**.
2. Select **Properties** and make sure that Display Notifications is disabled. When you have uploaded and configured the new template, come back to this view and restore the Display Notifications option to its original state.
3. Log into your Windows Server.
4. On your Windows server open the Group Policy Management Tool.
5. Navigate to the **Group Policy Object** you want to edit, right-click and select **Edit** to display the GPO Editor pane.
6. Select **Computer Configuration > Administrative Templates > Bradford Persistent Agent**.
7. In the pane on the right, right-click on the Balloon Notifications setting and select Properties.
8. On the **Setting** tab in the **Properties** window select **Not Configured** and click **OK**.
9. When all of your clients have received the updated settings, the new template can be installed.
10. Navigate to the **Group Policy Object** you want to edit, right-click and select **Edit** to display the GPO Editor pane.
11. Right-click **Computer Configuration > Administrative Templates** and select **Add/Remove Templates**, to show the current templates pop-up.
12. Select the old template and click **Remove**. Follow the instructions in the Install The Templates For GPO section shown above to install the new template.

Install an updated template

Occasionally new templates are made available to incorporate additional features. If you already have a Fortinet Administrative Template installed but it does not have Balloon Notifications enabled, follow the instructions below to update it. If you do have Balloon Notifications enabled, go to the previous section for instructions.



Before updating a template, be sure to record the current template settings. Existing template settings are lost when the new template is installed.

1. On your Windows server open the **Group Policy Management Tool**.
2. Navigate to the **Group Policy Object** you want to edit, right-click and select **Edit** to display the GPO Editor pane.
3. Right-click **Computer Configuration > Administrative Templates** and select **Add/Remove Templates**, to show the current templates pop-up.
4. Select the old template and click **Remove**. Follow the instructions in the Install The Templates For GPO section shown above to install the new template.

Modify settings

See the table below for settings which can be configured using the Administrative Templates provided.

Settings

Option	Definition
Persistent Agent template	
Host Name	Fully qualified host name of the FortiNAC Application Server or the FortiNAC Server if you are not using a pair. It is pushed out to the connecting host(s) to ensure that the Persistent Agent is communicating with the correct host in a distributed environment.
Balloon Notifications	Enables or Disables Balloon Notifications on a per-host or per-user basis. This setting is not required for configuring Server IP information. Options include: • Enabled: Forces balloon notifications for host state changes to be enabled on the host. • Disabled: Forces balloon notifications for host state changes to be disabled on the host. • Not Configured: Use the non-policy setting (Enabled).
Login Dialog	Enables or Disables the login dialog on a per-host or per-user basis. This setting is not required for configuring Server IP information. See Using Windows domain logon credentials on page 502 for further instructions. Options include: • Enabled: The login dialog is enabled. This can be used per-user to override a per-host setting of Disabled. • Disabled: The login dialog is disabled. The agent will never prompt the user for credentials. This is useful in certain Single-sign-on configurations. • Not Configured: The login dialog is enabled, unless overridden by a per-user configuration.
System Tray Icon	Enables or Disables the system tray icon on a per-host or per-user basis. This setting is not required for configuring Server IP information. (Requires Persistent Agent 2.2.3 or higher). Options include: • Enabled: The system tray icon is enabled. This can be used per-user to override a per-host setting of Disabled. • Disabled: The system tray icon is disabled. Disabling the system tray icon also

Option	Definition
	disables the following functionality: Status Notifications (Show Network Access Status, Login, Logout), Message Logs and the About dialog. • Not Configured: The system tray icon is enabled, unless overridden by a per-user configuration.
Max Connection Interval	The maximum number of seconds between attempts to connect to FortiNAC.
Persistent Agent security settings	
Security Mode	Indicates whether security is enabled or disabled.
Home Server	Server with which the agent always attempts to communicate first. Protocol configuration change requests are honored only when they are received from this server. If this servers is not set, it is automatically discovered using Server Discovery. On upgrade, this is populated by the contents of ServerIP.
Limit Connections To Servers	• Enabled: Agent communicates only with its Home Server and servers listed under Allowed Servers list displayed. • Disabled: Agent searches for additional servers when the home server is unavailable. • Allowed Servers List: In large environments there may be more than one set of FortiNAC servers. If roaming between servers is limited, list the FQDNs of the FortiNAC Application Servers or FortiNAC Servers with which the agent can communicate.
Passive Agent template	
Passive Agent	Server URL List: Comma separated list of URLs (HTTP(s)://<server_name>/<context> formatted) for the FortiNAC servers that hosts running an agent should contact. Hosts must be able to reach all of the URLs in order to run properly. Example: http://qa228/registration The context portion of the Server URL is the area of the captive portal the agents should contact, such as registration, remediation, or authentication.

Registry keys

The template setup shown in the table above modifies the Windows host's registry settings. The table below shows the modifications made to the host's registry keys by the Group Policy Object using the administrative template. If you use a tool other than GPO, you must make sure to set the appropriate keys on each host.

Upon installation of the Persistent Agent, the following key is created by default (and can be viewed using the Windows registry editor on the endstation):

```
HKLM\Software\Bradford Networks\Client Security Agent
```

When registry settings are pushed to a host via software, one or both of the following keys are created (depending upon the values pushed):

```
HKEY_USERS\ ... \Software\Policies\Bradford Networks\Persistent Agent
HKLM\Software\Policies\Bradford Networks\Persistent Agent
```



When the settings are pushed, the values for HKLM\Software\Bradford Networks\Client Security Agent will remain the same, but any settings altered via the software push will override those listed in the original key.



On 64-bit operating systems in RegEdit, these registry values will appear in the following key: HKLM\Software\wow6432node.

Key	Value	Data
Persistent Agent		
HKLM\Software\Policies\Bradford Networks\Persistent Agent	ServerIP	The fully qualified hostname to which the agent should communicate. Data Type: String Default: Not Configured
HKLM\Software\Policies\Bradford Networks\Persistent Agent	ClientStateEnabled	0: Do not show balloon notifications on status changes. 1: Show balloon notifications on status changes. Data Type: DWORD Default: Not Configured
HKEY_USERS\...\Software\Policies\Bradford Networks\Persistent Agent	ClientStateEnabled	0: Do not show balloon notifications on status changes. 1: Show balloon notifications on status changes. Data Type: DWORD Default: Not Configured
HKLM\Software\Policies\Bradford Networks\Persistent Agent	LoginDialogDisabled	0: Enable Login Dialog. 1: Disable Login Dialog. Data Type: DWORD Default: Not Configured (Login Dialog displayed)
HKEY_USERS\...\Software\Policies\Bradford Networks\Persistent Agent	LoginDialogDisabled	0: Enable Login Dialog. 1: Disable Login Dialog. Data Type: DWORD Default: Not Configured (Login Dialog displayed)
HKEY_USERS\...\Software\Policies\Bradford Networks\Persistent Agent	ShowIcon	0: Do not show the tray icon. 1: Show the tray icon. Data Type: DWORD Default: Not Configured (Tray icon displayed)

Key	Value	Data
HKLM\Software\Policies\Bradford Networks\Persistent Agent	ShowIcon	0: Do not show the tray icon. 1: Show the tray icon. Data Type: DWORD Default: Not Configured (Tray icon displayed)
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Bradford Networks\Persistent Agent	maxConnectInterval	The maximum number of seconds between attempts to connect to FortiNAC. Data Type: Integer Default: 960
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Bradford Networks\Persistent Agent	securityEnabled	0: Disable Agent Security. 1: Enable Agent Security Data Type: Integer Default: 1
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Bradford Networks\Persistent Agent	homeServer	The fully qualified hostname of the default server with which the agent should communicate. Data Type: String Default: Empty
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Bradford Networks\Persistent Agent	restrictRoaming	0: Do not restrict roaming. Allow agent to communicate with any server. 1: Restrict roaming to the home server and the allowed servers list. Data Type: Integer Default: 0
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Bradford Networks\Persistent Agent	allowedServers	Comma-separated list of fully qualified hostnames with which the agent can communicate. If restrict roaming is enabled, the agent is limited to this list. The home server does not need to be included in this list (for example, a.example.com, b.example.com, c.example.com). Data Type: String Default: Empty
Passive Agent		
HKEY_USERS\{SID}\Software\Policies\Bradford Networks\PASSIVE	ServerURL	Server URL List: Comma separated list of URLs for the FortiNAC servers that an agent should contact. Example:

Key	Value	Data
		http://qa228/registration The context portion of the Server URL is the area of the captive portal the agents should contact, such as registration, remediation, or authentication.
HKLM\Software\Policies\Bradford Networks\PASSIVE	ServerURL	Server URL List: Comma separated list of URLs for the FortiNAC servers that an agent should contact. Example: http://qa228/registration The context portion of the Server URL is the area of the captive portal the agents should contact, such as registration, remediation, or authentication.

Deploy the Passive Agent

1. On your Windows server open the Group Policy Management Tool.
2. Navigate to the Group Policy Object you want to edit.
3. Right-click the Group Policy Object and select **Edit** to display the GPO Editor pane.
4. Click **User Configuration > Policies > Windows > Settings Scripts (Logon/Logoff)** to display the Logon and Logoff script configurations.
5. Double click **Logon** for Logon Properties.
6. Click **Add** and then browse to the location of `FortiNAC_Passive_Agent.exe`.
7. Select `FortiNAC_Passive_Agent.exe` to add it to the Script Name field.
8. Enter **-logon** in the Script Parameters field.
9. Click **OK**.

To ensure the user is logged off the host upon logging out, do the following:

1. Follow steps 1-4, and then double-click **Logoff**.
2. Add `FortiNAC_Passive_Agent.exe` to the Script Name field, and then enter **-logoff** in the Script Parameter field.
3. Click **OK**.

Agent updates

To update FortiNAC, download the most recent FortiNAC software distribution. Connection settings must be configured for access to the server where the download is hosted.

The database is automatically backed up during the update process.

High availability environment

To update your servers in a high availability environment note the following:

- The primary server must be running and in control in order to update the system.
- The secondary server(s) must be running.
- The primary server must be able to communicate with the secondary server(s).
- The primary server automatically updates the secondary server(s).
- If the secondary server(s) is in control, FortiNAC prevents you from updating and displays a message with detailed instructions indicating that the Primary must be running and in control.
- If the secondary server is in a different platform, a different firmware image will need to be uploaded. The system will detect the secondary being on a different platform and prompt you to select a different image file.

Update the primary server following the instructions shown here for a regular update.

Update Managed Servers

FortiNAC Manager can be used to update the managed servers. This is done by propagating the update from the FortiNAC Manager to the managed servers throughout the environment.

Managed Server Update Requirements

Secondary servers must have an associated Primary server. If no Primary server is associated, change secondary server to a standalone in order to upgrade:

1. Go to **System > CA management**.
2. Select a managed CA and click **Edit** button at the top.
3. De-select Failover and click **OK**. The CA will appear under the Standalone Group
4. Wait several minutes until the Status shows "Running".

The CA is ready to upgrade.

Configure settings

Configure the connection settings for the download location so the Auto-Def Synchronizer, Agent packages, and the Software Distribution Updates can be completed. You need to change the default settings if another server is used to host the auto-definition or updated distribution files.

1. Click **System > Settings**.
2. Go to **Updates > Agent Packages > Agent Updates**.
3. Use the table below to enter the update settings.
4. Contact Customer Support for the correct login credentials.
5. Click **Test** to check that the settings allow connection to the auto-definition directory and the product distribution

directory.



Refer to the System Update Settings section of the Release Notes on our website for information about the distribution directory for the specific version you wish to download and install.

6. Once connection to the server is established, click **Ok**.

Settings

Field	Definition
Host	Host IP address, host name, or fully qualified name of the server that is hosting the updates. Applies to both software and Operating System updates.
Auto-Definition Directory	The sub-directory where the weekly antivirus and operating system updates are located. Default setting for this field is a period (.). If you are downloading these files from a server on your network, specify the directory containing the updates. If you prefer to download and install updates on a delayed schedule, you can choose system updates from one, two, three or four weeks ago by modifying this field with an additional sub-directory. For example, entering <code>/week1</code> gives you an update that is one week old. Available directories are: • <code>./week1</code> contains updates that are one week old. • <code>./week2</code> contains updates that are two weeks old. • <code>./week3</code> contains updates that are three weeks old. • <code>./week4</code> contains updates that are four weeks old.
Agent Distribution Directory	The sub-directory where the Agent update files are located. This field will vary depending on the version of the software being updated. A forward slash (/) may be required in the path configuration. Click Test to confirm the configuration. Refer to the FortiNAC Release Notes for information about the distribution directory for the specific version package you wish to download and install.
User	The user name for the connection.
Password	The password for the connection.
Protocol	Applies to both software and Operating System updates. • HTTP • HTTPS • SFTP - This option has been deprecated and no longer works. It will be removed in a future release. • FTP • PFTP
Buttons	
Test	Tests the connection between the FortiNAC program and the update server.
Revert To Defaults	Returns the window to the factory default settings.

System

Latest/All Upgrades

In **Latest** tab, it will show only the most current FortiNAC-OS firmware minor version that can be downloaded and install. For example, if the current version of FortiNAC is running in 7.6.x, only versions within 7.6.x are available.

In **All Upgrades** tab, all FortiNAC-OS firmware upgrades available can be download and install.



As of FortiNAC versions F 7.6.3 and greater, downloading the image is part of the upgrade process and not a separate step. This additional step increases the amount of time required to complete the upgrade.

To update the software on the appliance, download the distribution files to the appliance.

1. Click **System > Settings**.
2. Expand the **Updates** folder.
3. Select **System** from the tree.
4. Choose **Latest** or **All Upgrades** tab.
5. Choose a FortiNAC version and click **Upgrade**. FortiNAC automatically connects to the download server and retrieves a list of the files available for download. FortiNAC displays a warning message if no update files are found.
6. Wait for the firmware file to be downloaded and installed.
7. Verify that the update was successful by checking the version number for the currently installed version. This can be viewed using either the Admin UI or CLI.

1. **Admin UI:**

- System Summary Dashboard widget
- User icon drop-down menu in upper right corner

CLI: Enter the following at the command line prompt:

```
get system status
```

File Upload

FortiNAC-OS firmware upgrade can also be done manually by uploading the firmware file.

1. Click **System > Settings**.
2. Expand the **Updates** folder.
3. Select **System** from the tree.
4. Choose **File Upload** tab.
5. Click **+Browse** to upload the FortiNAC-OS firmware file.
6. Click **Upgrade** to continue with the installation.

User/Host Management

User/Host Management groups together global options for controlling user and host properties, such as aging or the number of hosts per user. Options include:

Option	Definition
Aging	Controls how long users and hosts remain in the database. See Aging on page 1006 .
Allowed Hosts	Controls the number of hosts that can be registered to an individual user in the database. See Allowed hosts on page 1008 .
Device Profiler	Enable or Disable creating rogues from DHCP packets heard on the network. See Device profiler on page 1008 .
MAC address Exclusion	Enable or Disable the option to ignore Microsoft LLTD and Multicast Addresses by FortiNAC when they connect to the network. These addresses will not be treated as rogues and will be allowed on the production network. See MAC address exclusion on page 1009 .

Aging

FortiNAC manages registered hosts, unregistered (rogue) hosts and users. The settings on the Aging view determine how long host and user records remain in the FortiNAC database.

Age times are used to calculate the Expiration Date and the Inactivity Date displayed on the **Host Properties** window. Age times for users are used to calculate the Expiration Date on the **User Properties** window for both network users and administrators that are not set to Never Expire. Modifying age times on this window does not affect those hosts, users or administrators whose Expiration and Inactivity date fields already contain data.

Once the specified time has elapsed for a record, it is removed from the database. These age times are global. Age times are applied to hosts and users as they are created and added to the database and to existing hosts, users with no aging values set. Age times are applied to administrators with no aging values set that do not have the Never Expire option enabled.

Administrators that are assigned the **System Administrator** profile cannot be aged out.

Adding age times to existing hosts or users with no age times can cause some hosts or users to be removed from the database immediately, depending on the creation date of the database record. If, for example, the host or user creation date is 01/01/2010, today's date is 02/02/2010 and Days Valid is set to 5, then the Expiration Date calculated is 01/06/2010. The record is deleted immediately because the calculated expiration date has already passed.

To reset dates on existing records, you must clear the dates using **Clear**. Then, enter new age times on this window and click **Save Settings**.

If users or hosts are set to never expire, clearing and resetting age times does not affect those records.

Age times can be overridden individually on the **User** or **Host Properties** window. The **Set Expiration** options on the **Properties** window allow you to set records to **Never Expire**. You can also use these settings to manage guests who will have access to the network for a limited time.

Aging a large number of hosts or users at the same time can cause processing delays with FortiNAC if users attempt to re-register within a short period of time of each other. It is recommended that you stagger the aging times to reduce the number of possible re-registrations at any given time.

1. Click **Users & Hosts > Settings**
2. Select **Aging** from the tree.
3. Modify the settings shown in the table below.
4. Click **Save Settings**.

Settings

Field	Definition
Days Valid	Number of days a host record remains in the FortiNAC database before it is deleted. Host records are created when the host initially connects and is registered with the network.
Days Inactive	Number of days a host can be inactive before the host record is deleted from the database.
Days Valid for Host Who has all adapters with randomized MAC	Specifies how long (in days) a host record is considered valid when all its adapters use randomized MAC addresses. This helps manage the lifecycle of privacy-focused devices that rotate MAC addresses.
Days inactive for Host who has all adapters with randomized MAC	Defines the number of consecutive days a host with only randomized MAC adapters must be absent from the network before its record is automatically removed from the database.
Clear Unregistered	Removes the Age Time Expiration Date and Inactivity Date that appears in the Host Properties for all unregistered hosts (i.e., a rogue).
Clear Registered	Removes the Age Time Expiration Date and Inactivity Date that appears in the Host Properties for all registered hosts, except those set to Never Expire. Clear Registered also removes the Age Time Expiration Date and Inactivity Date for registered hosts with age times set based on group membership or set individually. You must set individual and group based age times again after using Clear Registered .
Delete hosts registered to user upon expiration	If enabled, all hosts associated with a user are removed from the database when the user ages out of the database.
Days Valid (Users)	Number of days a user record remains in the FortiNAC database before it is deleted. User records are created when the user registers a host.
Days Inactive (Users)	Number of days a user can be inactive before the user record is deleted from the database.
Clear Aging Values for All Users	Removes the Age Time Expiration Date that appears in the User Properties for all users, except those set to Never Expire.

The date on which the host record will be removed from the database is displayed in [Properties on page 221](#). The date on which the user record will be removed from the database is displayed in [User properties on page 200](#). The date on which an administrator will be removed from the database is displayed in [Administrators on page 119](#).

Administrators never expire under any circumstances. These users must be removed manually from the **Admin Users** view.

If you leave these fields empty, global aging is disabled. Setting the value to zero causes the record to be removed the next time the server polls the network. See [Aging out host or user records on page 241](#) for additional information on aging.

Allowed hosts

Use allowed hosts to configure the maximum hosts a single user can register.

Field	Definition
Allowed Host Records	Number of registered hosts a single user may have. For example, if a user has three (3) hosts and the limit is set to two (2), only two of the hosts can be registered on the network. Either "Over Registered Limit" or "Registration Failed" is displayed when count has been exceeded. This field can be modified for a single user on the user view. If Allowed Hosts is set under Add or Modify user, the default setting here is ignored. Default = 1000 See Add or modify a user on page 202.

1. Click **System > Settings**.
2. Expand the **User/Host Management** folder.
3. Select **Allowed Hosts** from the tree.
4. Enter the maximum number of hosts a user can register.
5. Click **Save Settings**.

Device profiler

Controls creation of rogue hosts from DHCP packets heard on the network.

Field	Definition
Create Rogues from DHCP packets	When enabled, rogues will be created from information learned from DHCP packets heard on the network. It helps to quickly learn about hosts communicating on the network, but in some network environments it can add a large number of rogues hosts from unmanaged areas of the network. Default = true  FortiNAC-OS Requirement: "set allowaccess" command option "dhcp". See Open ports for details.

Field	Definition
Perform Active (NMAP) profiling without ICMP ping	When enabled, Active NMAP scans will not perform a ICMP ping of the host prior to initiating the NMAP scan. This allows networks where ICMP is blocked to still do NMAP scanning. This is disabled by default as it could be a considerable performance drain scanning a large number of uncontactable hosts. Default = false
FortiGuard IoT Query URL	The URL for the API to which FortiNAC must connect to query IoT data from the FortiGuard IoT service. This information is used when profiling IoT devices using the Device Profiler method "FortiGuard". For a list of possible servers, click the "?" button next to the option.
Enable FortiGuard IoT Collect Service	When enabled, FortiNAC sends DHCP fingerprint information collected from IoT devices on the network to the FortiGuard IoT service. This improves the query results when profiling devices using the "FortiGuard" Device Profiler method.
Proactive "Active" method profiling	Enable this to automatically active endpoint (NMAP) fingerprints. User doesn't need to create a device profiling rule to identify devices
Proactive "Fortiguard" method profiling	Enable this to automatically create Fortiguard fingerprints. User doesn't need to create a device profiling rule to identify devices.
FortiGuard Collect URL	The URL for the API to which FortiNAC must connect to send IoT data. For a list of possible servers, click the "?" button next to the option. The possible servers are: Anycast: globaldevcollect.fortinet.net usdevcollect.fortinet.net eudevcollect.fortinet.net AWS: globaldevcollect2.fortinet.net usdevcollect2.fortinet.net eudevcollect2.fortinet.net Note: Users can input URL based on their region. For example, users from the European Union can use the URL with eu.

1. Click **System > Settings**.
2. Expand the **User/Host Management** folder.
3. Select **Device Profiler** from the tree.
4. Use the check boxes to enable or disable the desired functions.
5. Enter into the field the desired URL for the FortiGuard IoT service. For a list of options, click to the "?" button next to the field.
6. Click **Save Settings**.

MAC address exclusion

MAC address Exclusion allows you to add Microsoft LLTD Addresses and Multicast Addresses to a list of addresses that will be ignored when they connect to the network. If a device or host with one of these MAC addresses connects to the network, FortiNAC ignores the connection and allows the host or device onto the production network.

Excludes addresses within the IANA IPv4 multicast range 01:00:EE:00:00:00 to 01:00:5E:7F:FF:FF and within the IANA IPv6 multicast range 33-33-00-00-00-00 to 33-33-FF-FF-FF-FF.

An event, "Found Ignored MAC address", is generated each time a host or device connects with a MAC address in this list. Configure an alarm for the event with email notification to alert Administrators. The event can also be disabled if notification is unnecessary.

Default settings

This feature is set by default to ignore Microsoft LLTD and Multicast MAC addresses indefinitely. When any MAC address connects that falls within either the Microsoft LLTD or Multicast address range FortiNAC does the following:

- Creates a "Found Microsoft LLTD or Multicast Address" event and an alarm alerting the administrator that FortiNAC has seen a Microsoft LLTD or Multicast address on the network for the first time. This critical alarm warns administrators that if these addresses should continue to be ignored, they must configure the MAC address Exclusions list or the MAC addresses will be treated as rogues.
- A timer is set that expires in 48 hours.
- While that timer is active, FortiNAC continues to ignore Microsoft LLTD and Multicast MAC addresses. Events and alarms continue to be created for each connection from one of these MAC addresses.
- If the administrator has not configured the MAC address Exclusions, when the 48 hour timer expires FortiNAC no longer ignores Microsoft LLTD and Multicast MAC addresses. FortiNAC creates rogues for each MAC address that connects, just as it would any other MAC address.



Administrators can configure MAC address Exclusion at any time to include or exclude Microsoft LLTD and Multicast MAC addresses. As soon as settings have been modified, the default behavior described above stops and the new settings take effect.

Configure exclusion list

1. Click **System > Settings**.
2. Expand the **User/Host Management** folder.
3. Select **MAC address Exclusion** from the tree.
4. Use the Exclude Microsoft LLTD Addresses and Exclude Multicast Addresses check boxes to add or remove those ranges from the Address Range table.
5. Changes are saved immediately.

Settings

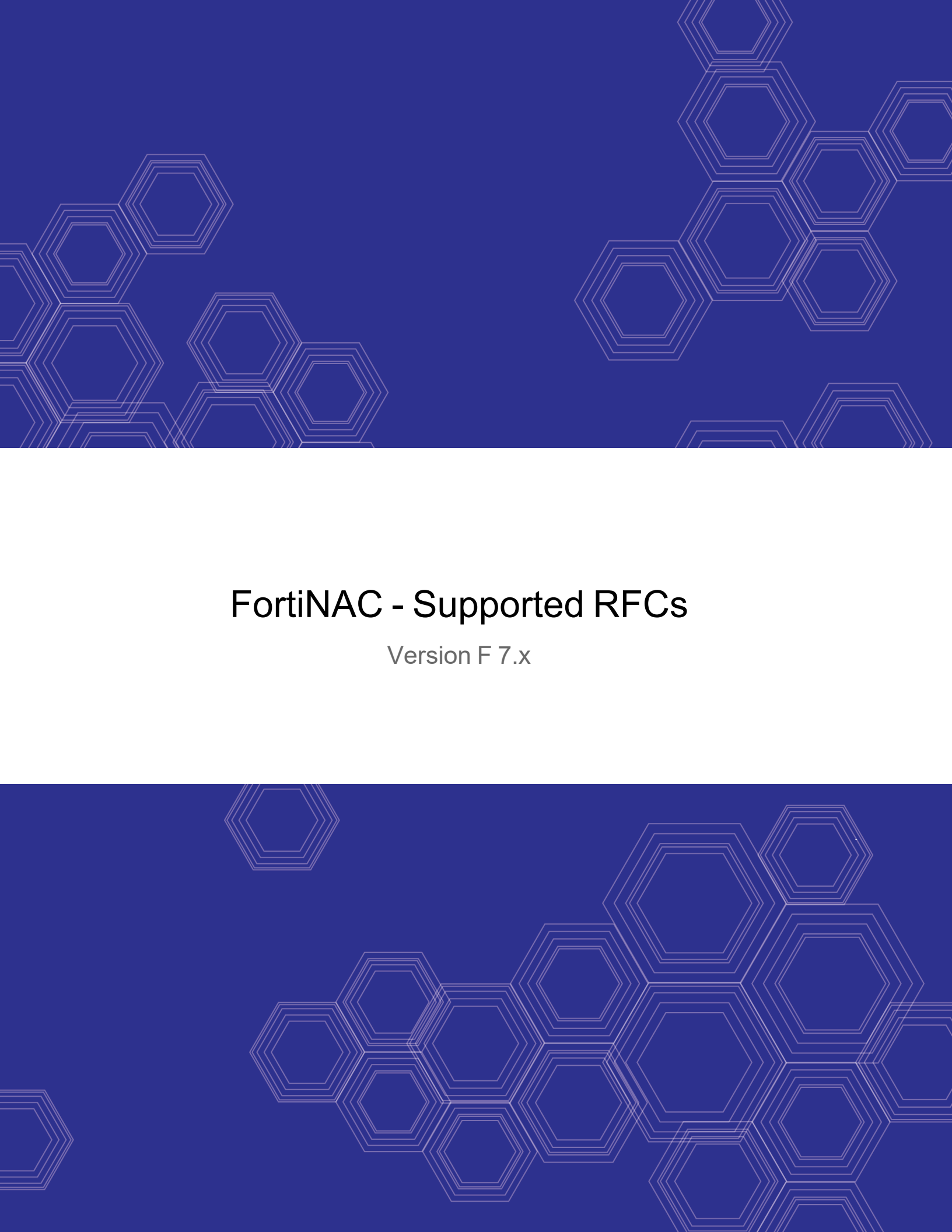
Field	Definition
Exclude Microsoft LLTD Addresses	If enabled, adds the complete range of Microsoft LLTD MAC addresses to the Excluded MAC address Ranges table ensuring that the correct range has been entered.
Exclude Multicast Addresses	If enabled, adds the complete range of Multicast MAC addresses to the Excluded MAC address Ranges table ensuring that the correct range has been entered.

Change log

Date	Change description
1-8-2026	Bug ID 1240812
8-12-2024	Bug ID 1040797



Copyright© 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.



FortiNAC - Supported RFCs

Version F 7.x

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com

April 28, 2024

FortiNAC F 7.x Supported RFCs

49-20-748677-20210922

TABLE OF CONTENTS

Supported RFCs	4
Cryptography	5
DHCP	6
DHCP is used in the following modules:	6
DNS	7
DNS is used in the following modules:	7
ICMP	8
ICMP is used in the following Modules:	8
IP	9
IP Multicast	10
IPv4	11
IPv4 is used in the following Modules:	11
IPv6	12
IPv6 is used in the following Modules:	12
LDAP	13
LDAP is used in the following Modules::	13
NAT	14
RADIUS	15
RADIUS is used in the following Modules:	15
SFTP	16
SFTP is used in the following Modules:	16
SNMP	17
SNMP is used in the following Modules:	17
SSH	19
SSH is used in the following Modules:	19
SSL	20
Syslog Protocol	21
Syslog is used in the following modules:	21
TCP	22
TLS	23
TLS is used in the following modules:	23
UDP	24
VPN	25
FortiNAC Portal Configuration includes VPN related settings for VPN access:	25
Wireless	26
Wireless Security is used in the following modules:	26
Other Protocols	27
Miscellaneous	28

Supported RFCs

FortiNAC supports the following RFCs:

Cryptography on page 5	LDAP on page 13	TCP on page 22
DHCP on page 6	NAT on page 14	TLS on page 23
DNS on page 7	RADIUS on page 15	UDP on page 24
ICMP on page 8	SFTP on page 16	VPN on page 25
IP on page 9	SNMP on page 17	Wireless on page 26
IP Multicast on page 10	SSH on page 19	Other Protocols on page 27
IPv4 on page 11	SSL on page 20	Miscellaneous on page 28
IPv6 on page 12	Syslog Protocol on page 21	

Cryptography

[RFC 7627](#): Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension

[RFC 2315](#): PKCS #7: Cryptographic Message Syntax Version 1.5

[RFC 1321](#): The MD5 Message-Digest Algorithm

MD5 is used in SNMP as authentication protocol, and can be found in the following:

Settings > System Communication > SNMP

Network > Inventory > Credentials

Network > Inventory > Add Devices

Network > Inventory > Customer > Containers > Start Discovery

PKCS #7 is a standard syntax for storing signed and/or encrypted data, can be found in the following:

System > Certificate Management > Generate CSR

DHCP

[RFC 2132](#): DHCP Options and BOOTP Vendor Extensions

[RFC 2131](#): Dynamic Host Configuration Protocol

[RFC 3633](#): IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6

[RFC 3315](#): Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

DHCP is used in the following modules:

Systems > Config Wizard

Systems > Settings > User/Host Management > Device Profiler > method

Systems > Settings > Controls > Access Point Management

DNS

[RFC 1034](#): Domain Names - Concepts and Facilities

[RFC 1035](#): Domain Names - Implementation and Specification

[RFC 1982](#): Serial Number Arithmetic

[RFC 2181](#): Clarifications to the DNS Specification

DNS is used in the following modules:

System > Settings > Control > Allowed Domains

System > Config Wizard

[Agent server discovery](#)

Systems > Settings > Controls > Access Point Management

Network > RADIUS > Winbind

ICMP

[RFC 792](#): Internet Control Message Protocol

[RFC 1191](#): Path MTU Discovery

[RFC 4884](#): Extended ICMP to Support Multi-Part Messages

[RFC 6633](#): Deprecation of ICMP Source Quench Messages

[RFC 6918](#): Formally Deprecating Some ICMPv4 Message Types

[RFC 4443](#): Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification

ICMP is used in the following Modules:

Systems > Settings > User/Host Management > Device Profiler

Network > Inventory > Add Container

IP

[RFC 4301](#): Security Architecture for the Internet Protocol

[RFC 3272](#): Overview and Principles of Internet Traffic Engineering

[RFC 2072](#): Router Renumbering Guide

[RFC 2071](#): Network Renumbering Overview: Why would I want it and what is it anyway?

[RFC 2003](#): IP Encapsulation within IP

[RFC 1918](#): Address Allocation for Private Internets

[RFC 1123](#): Requirements for Internet Hosts -- Application and Support

[RFC 1122](#): Requirements for Internet Hosts -- Communication Layers

[RFC 791](#): Internet Protocol

IP Multicast

[RFC 2365](#): Administratively Scoped IP Multicast

[RFC 1112](#): Host Extensions for IP Multicasting

[RFC 3306](#): Unicast-Prefix-based IPv6 Multicast Addresses

FortiNAC provides capability to exclude Multicast addresses under MAC Address Exclusion, it can be found under:

System > Setting > User/Host Management > MAC Address Exclusion

IPv4

[RFC 791](#): Internet Protocol - RFC Editor

[RFC 4632](#): Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan

IPv4 is used in the following Modules:

System > Settings > System Communication > Address

User & Hosts > Adapters > IP address(All IPs)

Network > Inventory > Add container

Systems > Config Wizard

System > Settings > System Management > High Available

IPv6

[RFC 2464](#) – Transmission of IPv6 Packets over Ethernet Networks

[RFC 1885](#) – Internet Control Message Protocol (ICMPv6) for IPv6 (OBSOLETE)

[RFC 2460](#): Internet Protocol, Version 6 (IPv6) Specification

[RFC 4291](#): IP Version 6 Addressing Architecture

IPv6 is used in the following Modules:

Supported for IPv6	Not Supported for IPv6
Portal communication (eth1)	Device management in Inventory (Creation/discovery of network devices)
Admin UI access (eth0)	
Agent communication	
L3 polling IPv6 addresses displayed in the Host View and Adapter View	

LDAP

[RFC 4511](#): Lightweight Directory Access Protocol (LDAP) - The Protocol

[RFC 4513](#): Lightweight Directory Access Protocol (LDAP) - Authentication Methods and Security Mechanisms

[RFC 4512](#): Lightweight Directory Access Protocol (LDAP) - Directory Information Models

LDAP is used in the following Modules::

Global > Settings > Authentication > LDAP

Policy & Objects > Authentication > Configuration > Authentication methods

Portal > Portal Configuration > Global > Global Properties > Settings > Login Type Options

System > Settings > Persistent Agent > Credential Configuration

Users & Hosts > Administrators

NAT

[RFC 7857](#): Updates to Network Address Translation (NAT) Behavioral Requirements

[RFC 5508](#): NAT Behavioral Requirements for ICMP

[RFC 4787](#): Network Address Translation (NAT) Behavioral Requirements for Unicast UDP

[RFC 3022](#): Traditional IP Network Address Translator (Traditional NAT)

[RFC 5382](#): NAT Behavioral Requirements for TCP

FortiNAC provides capability for NAT Detection by examining devices IP address, and IP ranges can be configured at the following:

System > Setting > Identification > NAT Detection

RADIUS

[RFC 2548](#): Microsoft Vendor-specific RADIUS Attributes

[RFC 2866](#): RADIUS Accounting

[RFC 3576](#): Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)

[RFC 3580](#): IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines

[RFC 5176](#): Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)

[RFC 6614](#): Transport Layer Security (TLS) Encryption for RADIUS

[RFC 6613](#): RADIUS over TCP

[RFC 5176](#): CoA/Disconnect Message Cookbook

RADIUS is used in the following Modules:

Global > Settings > Authentication > Roaming Guest

Policy & Objects > Authentication > Configuration > Authentication methods

Portal > Portal Configuration > Global > Global Properties > Settings > Login Type Options

System > Settings > Persistent Agent > Credential Configuration

Users & Hosts > Administrators.

Network > RADIUS

Network > Network events

Systems > Settings > User/Host Management > Device Profiler > Method

SFTP

[RFC 913](#): Simple File Transfer Protocol - RFC Editor

[RFC 959](#): File Transfer Protocol

[RFC 4253](#): The Secure Shell (SSH) Transport Layer Protocol

SFTP is used in the following Modules:

System > Settings > System Management > Remote Backup Configuration

System > Settings > Updates-System > Protocols

SNMP

[RFC 1155](#): Structure and Identification of Management Information for TCP/IP-based Internets

[RFC 1156](#): Management Information Base for Network Management of TCP/IP-based internets

[RFC 1157](#): A Simple Network Management Protocol (SNMP)

[RFC 1158](#): Management Information Base for Network Management of TCP/IP-based internets:MIB-II

[RFC 1212](#): Concise MIB Definitions

[RFC 1213](#): Management Information Base for Network Management of TCP/IP-based internets:MIB-II

[RFC 1215](#): A Convention for Defining Traps for use with the SNMP

[RFC 1493](#): Definitions of Managed Objects for Bridges

[RFC 2578](#): Structure of Management Information Version 2 (SMIv2)

[RFC 2674](#): Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions

[RFC 2863](#): The Interfaces Group MIB

[RFC 3410](#): Introduction and Applicability Statements for Internet Standard Management Framework

[RFC 3411](#): An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks

[RFC 3412](#): Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)

[RFC 3413](#): Simple Network Management Protocol (SNMP) Applications

[RFC 3414](#): User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)

[RFC 3416](#): Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)

[RFC 3417](#): Transport Mappings for the Simple Network Management Protocol (SNMP)

[RFC 3635](#): Definitions of Managed Objects for the Ethernet-like Interface Types

[RFC 4022](#): Management Information Base for the Transmission Control Protocol (TCP)

[RFC 4113](#): Management Information Base for the User Datagram Protocol (UDP)

[RFC 4293](#): Management Information Base for the Internet Protocol (IP)

SNMP is used in the following Modules:

Settings > System Communication > SNMP

System > Settings >System Communication >Trap MIB Files

Network > Inventory

System > Settings->System Communication > Log Receivers

Systems > Settings > User/Host Management > Device Profiler > Method

Network > L2 Polling

SSH

[RFC 4250](#): SSH Assigned Numbers

[RFC 4251](#): SSH Protocol Architecture

[RFC 4252](#): SSH Authentication Protocol

[RFC 4253](#): SSH Transport Layer Protocol

[RFC 4254](#): SSH Connection Protocol

SSH is used in the following Modules:

System > Settings > System Management > Remote Backup Configuration

Network > Inventory > Add device

Systems > Settings > User/Host Management > Device Profiler > method

SSL

[RFC 6176](#): Prohibiting Secure Sockets Layer (SSL) Version 2.0

[RFC 6101](#): The Secure Sockets Layer (SSL) Protocol Version 3.0

Syslog Protocol

[RFC 3164](#): The BSD Syslog Protocol

[RFC 5424](#): The Syslog Protocol

Syslog is used in the following modules:

Settings > System Communication > Syslog Files and Log Receivers

<https://docs.fortinet.com/document/fortinac/9.4.0/administration-guide/880398/syslog-files>

<https://docs.fortinet.com/document/fortinac-f/7.2.0/administration-guide/499308/log-events-to-an-external-log-host>

Logs > Events & Alarms

<https://docs.fortinet.com/document/fortinac-f/7.2.0/administration-guide/338223/examples-of-syslog-messages>

TCP

[RFC 1006](#): ISO Transport Service on top of the TCP Version: 3

[RFC 6691](#): TCP Options and Maximum Segment Size (MSS)

[RFC 6298](#): Computing TCP's Retransmission Timer

[RFC 6093](#): On the Implementation of the TCP Urgent Mechanism

[RFC 793](#): Transmission Control Protocol

TLS

[RFC 4680](#): TLS Handshake Message for Supplemental Data

[RFC 4681](#): TLS User Mapping Extension

[RFC 5246](#): The Transport Layer Security (TLS) Protocol Version 1.2

[RFC 5425](#): Transport Layer Security (TLS) Transport Mapping for Syslog

[RFC 5746](#): Transport Layer Security (TLS) Renegotiation Indication Extension

[RFC 6066](#): Transport Layer Security (TLS) Extensions: Extension Definitions

[RFC 6347](#): Datagram Transport Layer Security Version 1.2

[RFC 7858](#): Specification for DNS over Transport Layer Security (TLS)

[RFC 8446](#): The Transport Layer Security (TLS) Protocol Version 1.3

TLS is used in the following modules:

System > Settings > Persistent Agent > Transport Configuration

Network > Radius > Virtual servers > TLS details

Network > Service Connectors > Create New > Email Server

UDP

[RFC 768](#): User Datagram Protocol

VPN

[RFC 4026](#): Provider Provisioned Virtual Private Network (VPN) Terminology

[RFC 4110](#): A Framework for Layer 3 Provider-Provisioned Virtual Private Networks (PPVPNs)

[RFC 4111](#): Security Framework for Provider-Provisioned Virtual Private Networks (PPVPNs)

FortiNAC Portal Configuration includes VPN related settings for VPN access:

Portal > Portal Configuration > Create New / Edit > Configuration > VPN

Host Policy can also specified if Host is VPN Client:

Hosts > Policy Detail > Edit > Host > VPN Client

Wireless

[RFC 5415](#): Control and Provisioning of Wireless Access Points (CAPWAP)

[RFC 5416](#): Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11

[RFC 5417](#): CAPWAP Access Controller DHCP Option

[RFC 8110](#): Opportunistic Wireless Encryption (OWE)

Wireless Security is used in the following modules:

1. **Policy > Policy Configuration > Supplicant EasyConnect > Configuration > System > Quick Start > Network Settings > Network Devices > Wireless Security**
2. **System > Quick Start > Network Settings > Network Devices > Wireless Security**

Other Protocols

[RFC 7541](#): HPACK: Header Compression for HTTP/2

[RFC 7540](#): Hypertext Transfer Protocol Version 2 (HTTP/2)

[RFC 6887](#): Port Control Protocol (PCP)

[RFC 5905](#): Network Time Protocol Version 4: Protocol and Algorithms Specification

[RFC 2784](#): Generic Routing Encapsulation (GRE)

[RFC 1413](#): Identification Protocol

[RFC 1305](#): Network Time Protocol (Version 3) Specification, Implementation and Analysis

[RFC 1011](#): Official Internet Protocols

[RFC 959](#): File Transfer Protocol (FTP)

[RFC 862](#): Echo Protocol

Miscellaneous

[RFC 4470](#): Minimally Covering NSEC Records and DNSSEC On-line Signing—related to DNS

[RFC 3985](#): Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture

[RFC 3954](#): Cisco Systems NetFlow Services Export V9

[RFC 2780](#): IANA Allocation Guidelines For Values In the Internet Protocol and Related Headers

[RFC 1945](#): Hypertext Transfer Protocol -- HTTP/1.0

[RFC 950](#): Internet Standard Subnetting Procedure

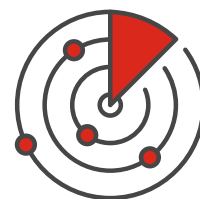
[RFC 905](#): ISO Transport Protocol Specification ISO DP 8073

[RFC 894](#): A Standard for the Transmission of IP Datagrams over Ethernet Networks



Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

FortiNAC



Welcome to the Fortinet FortiNAC Ordering Guide. This guide is designed to help customers understand and navigate the various options available for deploying Fortinet's network access control solution. FortiNAC enhances the Fortinet Security Fabric with comprehensive visibility, robust control, and automated response capabilities for everything that connects to your network. It also enables the implementation of microsegmentation policies and configuration changes across switches and wireless products from a wide range of vendors.

This guide outlines:

- Key FortiNAC capabilities, including network discovery, device profiling, authentication (Captive Portal, RADIUS), user and guest management, BYOD/onboarding, endpoint compliance, and automated control features like rogue device detection and firewall segmentation.
- Details on FortiCare offerings, which provide essential support services such as firmware updates, weekly network device database updates (supporting over 2400 devices), and access to the FortiGuard IoT Service for cloud-based device identification.
- Information on simplified licensing packages, including PLUS (entry-level with endpoint visibility, dynamic VLAN steering, advanced NAC, automated provisioning) and PRO (all PLUS features with enhanced visibility, control, and response).
- Options for perpetual and subscription licenses, available in various endpoint ranges (e.g., 100, 1000, 10000, 50000 endpoints).
- Details on FortiNAC hardware appliances (e.g., FNC-CA-500F, FNC-CA-600F, FNC-CA-700F, FNC-M-550F) and virtual appliances, categorized by network port capacity for SMB, Mid Enterprises, and Large Enterprises.
- Mandatory FortiCare SKUs for endpoint licensing and for activating support for hardware/VMs.
- Available Professional Services (e.g., FortiNAC Professional Service) and QuickStart Services for deployment assistance.

Product Offerings

FortiNAC is available with the following FortiCare offerings:

FortiCare Services

As a customer's business rapidly evolves, advancing its security capabilities is critical as well. Often, the customer does not have expertise within their organization to deploy, operate, and maintain these new capabilities or are up against tight deadlines to implement change. Fortinet understands this challenge and helps thousands of organizations every year tackle this problem with FortiCare Services. Fortinet's experts provide accelerated implementation of the customer's technology, reliable assistance through advanced support, and proactive care to ensure the customer's success with Fortinet investment. No matter the size or location of the customer's organization, Fortinet is ready to provide the customer with an elevated experience to help them achieve their business goals with superior security and performance.

FortiCare Support

A FortiCare Support contract entitles the customer not only to receive updates to the FortiNAC firmware, but also receive the following important feeds:

- **Network device database update:** FortiNAC supports more than 2400 switching, wireless, or firewall devices on the market. As new devices release, FortiNAC's network device database updates to reflect these new models. The weekly update from the FortiNAC team keeps the customer's deployment up to date.
- **FortiGuard IoT Service:** a method that FortiNAC has to identify devices is to use the cloud lookup service that FortiGuard Labs hosts. A FortiCare Support contract entitles the customer to use that service at no additional cost, giving them access to a database of millions of devices.

License Package

FortiNAC offer the broad features and deep integration capabilities through two licensing tiers: PLUS and PRO:

- **PLUS:** powerful and comprehensive features with the entry-level licensing package, provides endpoint visibility and dynamic VLAN steering, advanced network access controls, and automated provisioning for users, guests, and devices.
- **PRO:** includes all PLUS features and increases the level, providing the ultimate visibility, control, and response.

With the perpetual and subscription licensing pricing changes, the new FortiNAC-F hardware appliances had their prices revised due to Fortinet's new production of these appliances. With a production cost reduction, we can deliver cost savings for our customers without affecting performance and scalability.



Product Offerings

			PLUS	PRO
Visibility	Network	Network Discovery	✓	✓
		Rogue Identification	✓	✓
		Device Profiling and Classification	✓	✓
	Endpoint	Enhanced Visibility	✓	✓
		Anomaly Detection	✓	✓
		MDM Integration	✓	✓
		Persistent Agent	✓	✓
	User	Authentication	✓	✓
		Captive Portal	✓	✓
Automation/Control		Network Access Policies	✓	✓
		IoT Onboarding with Sponsor	✓	✓
		Rogue Device Detection and Restriction	✓	✓
		Firewall Segmentation	✓	✓
		MAC Address Bypass	✓	✓
		Full RADIUS (EAP)	✓	✓
		BYOD/Onboarding	✓	✓
		Guest Management	✓	✓
		Endpoint Compliance	✓	✓
		Web and Firewall Single Sign-on	✓	✓
Incident Response		Event Correlation		✓
		Extensible Actions and Audit Trail		✓
		Alert Criticality and Routing		✓
		Guided Triage Workflows		✓
Integrations		Inbound Security Events		✓
		Outbound Security Events	✓	✓
		REST API	✓	✓
Reporting		Customizable Reports	✓	✓

Ordering Information

	PLUS	PRO
PERPETUAL LICENSES*		
100 Endpoints	LIC-FNAC-PLUS-100	LIC-FNAC-PRO-100
1000 Endpoints	LIC-FNAC-PLUS-1K	LIC-FNAC-PRO-1K
10000 Endpoints	LIC-FNAC-PLUS-10K	LIC-FNAC-PRO-10K
50000 Endpoints	LIC-FNAC-PLUS-50K	LIC-FNAC-PRO-50K
SUBSCRIPTION LICENSES**		
100 Endpoints	FC5-10-FNAC1-213-01-DD	FC5-10-FNAC1-209-01-DD
1000 Endpoints	FC6-10-FNAC1-213-01-DD	FC6-10-FNAC1-209-01-DD
10000 Endpoints	FC7-10-FNAC1-213-01-DD	FC7-10-FNAC1-209-01-DD
50000 Endpoints	FC8-10-FNAC1-213-01-DD	FC8-10-FNAC1-209-01-DD
HARDWARE APPLIANCES		
SMB (up to 15000 managed endpoints)	FNC-CA-500F	
Mid Enterprises (up to 30000 managed endpoints)	FNC-CA-600F	
Large Enterprises (up to 50000 managed endpoints)	FNC-CA-700F	
Management Appliance (up to 100 FortiNAC-F CA)	FNC-M-550F	

* FortiCare SKUs for endpoint licensing are mandatory for activate the support for endpoint devices.

** You must purchase the FortiNAC model (hardware or VM) along with the corresponding FortiCare for the hardware/VM. Once purchased, you may add the desired subscription pack. The minimum order quantity for a subscription is 100 endpoint licenses, which includes FortiCare Premium Support.



Ordering Information

VIRTUAL APPLIANCES	
SMB (up to 15000 managed endpoints)	
Mid Enterprises (up to 30000 managed endpoints)	FNC-CAX-VM
Large Enterprises (up to 50000 managed endpoints)	
Management Appliance (up to 100 FortiNAC-F CA)	FNC-MX-VM

PLUS	PRO
PROFESSIONAL SERVICES	
FortiNAC Professional Service (FortiCare contract per day)	FP-10-PS001-830-01-01
QUICKSTART SERVICES	
FortiNAC QuickStart Deployment - Standard	
FortiNAC QuickStart Deployment - Advanced	

HARDWARE APPLIANCES				
HARDWARE MODEL	FORTINAC 500 NETWORK CONTROL AND APPLICATION SERVER WITH RAID AND REDUNDANT POWER SUPPLIES FOR UP TO 15000 MANAGED ENDPOINTS	FORTINAC 600 HIGH PERFORMANCE NETWORK CONTROL AND APPLICATION SERVER WITH RAID AND REDUNDANT POWER SUPPLIES FOR UP TO 30000 MANAGED ENDPOINTS	FORTINAC 700 ULTRA HIGH PERFORMANCE NETWORK CONTROL AND APPLICATION SERVER WITH RAID AND REDUNDANT POWER SUPPLIES FOR UP TO 50000 MANAGED ENDPOINTS	FORTINAC MANAGER 550 NETWORK MANAGER WITH RAID AND REDUNDANT POWER SUPPLIES
Hardware Product	FNC-CA-500F	FNC-CA-600F	FNC-CA-700F	FNC-M-550F
24x7 FortiCare Contract	FC-10-NF500-247-02-DD	FC-10-NF600-247-02-DD	FC-10-NF700-247-02-DD	FC-10-NF550-247-02-DD
Next Day Delivery Premium RMA Service (Requires 24x7 or ASE FortiCare)	FC-10-NF500-210-02-DD	FC-10-NF600-210-02-DD	FC-10-NF700-210-02-DD	FC-10-NF550-210-02-DD
4-hour Hardware Delivery Premium RMA Service (Requires 24x7 or ASE FortiCare)	FC-10-NF500-211-02-DD	FC-10-NF600-211-02-DD	FC-10-NF700-211-02-DD	FC-10-NF550-211-02-DD
4-Hour Hardware and Onsite Engineer Premium RMA Service (Requires 24x7 or ASE FortiCare)	FC-10-NF500-212-02-DD	FC-10-NF600-212-02-DD	FC-10-NF700-212-02-DD	FC-10-NF550-212-02-DD

VIRTUAL APPLIANCES		
VM MODEL	FORTINAC CONTROL AND APPLICATION NEXT-GEN VM SERVER SUPPORTS UP TO 50000 ENDPOINT DEVICES.	FORTINAC MANAGER NEXT-GEN VM SERVER SUPPORTS UP TO 100 CA SERVERS.
VM Product	FNC-CAX-VM	FNC-MX-VM
24x7 FortiCare Contract	FC-10-FNVXA-248-02-DD	FC-10-FNVXM-248-02-DD

SUPPORTED ENVIRONMENTS	
HYPERVERSORS	CLOUD MARKETPLACE
VMWARE ESXI	MICROSOFT AZURE
MICROSOFT HYPER-V	AMAZON AWS
NUTANIX	GOOGLE GCP
LINUX KVM	ORACLE OCI
	ALIBABA CLOUD

The number of FortiCare licenses must match the quantity of endpoint perpetual licenses (PRO or PLUS).

FORTICARE SUPPORT FOR FORTINAC PERPETUAL LICENSES	
LICENSE MODEL	
24x7 FortiCare Contract (100 Endpoints) for FortiNAC PLUS deployments	FC2-10-FNAC0-240-02-DD
24x7 FortiCare Contract (100 Endpoints) for FortiNAC PRO deployments	FC3-10-FNAC0-240-02-DD



Ordering Information

The following shows options for perpetual licensing upgrade:

FORTINAC PERPETUAL ONLY – UPGRADE LICENSING	
UPGRADE PATH	
BASE to PLUS Licensing Upgrade for 100 concurrent endpoint devices	FNC-LIC-BASE-UPG-100
PLUS to PRO Licensing Upgrade for 100 concurrent endpoint devices	FNC-LIC-PLUS-UPG-100
BASE to PRO Licensing Upgrade for 100 concurrent endpoint devices	FNC-LIC-PRO-UPG-100

SUPPORTED TRANCEIVERS LIST (HARDWARE APPLIANCES)	
DESCRIPTION	
1GE SFP SX transceiver module for systems with SFP and SFP/SFP+ slots	FN-TRAN-SX
1GE SFP LX transceiver module, 10km range, -40C to 85C, over SMF, for systems with SFP and SFP/SFP+ slots	FN-TRAN-LX
1GE SFP RJ45 transceiver module for systems with SFP and SFP/SFP+ slots	FN-TRAN-GC
10GE SFP+ transceiver module, short range for systems with SFP+ and SFP/SFP+ slots	FN-TRAN-SFP+SR
10GE SFP+ transceiver module, 10km long range for systems with SFP+ and SFP/SFP+ slots	FN-TRAN-SFP+LR



Fortinet Training and Certification

FCP - FortiNAC Training and Certification

Learn how to leverage the powerful and diverse capabilities of FortiNAC, using best practices for achieving visibility, control, and response. These fundamentals provide you with a solid understanding of how to implement network visibility and security automation.

Training Offering

For training SKUs, purchasing, and delivery options, see:

https://training.fortinet.com/local/staticpage/view.php?page=purchasing_process

Bill of Material Exercises

Exercise 1

Opportunity: New business

Customer segment: Manufacturing

Locations: Factories in 12 cities across the U.S.

Features needed: Visibility only of the network (e.g., PLC controllers, devices, PCs, unmanaged hubs, and switches)

Infrastructure: Two Azure datacenters, 12 Azure-connected sites with all Cisco hardened switches, a FortiGate firewall at the edge, and Meraki APs for wireless.

Number of devices: 8400

Terms: Three-year due to availability of capital expense money in this year's budget

Here is the proposed bill of material (BoM) using VM, with three-year term and support:

	PART NUMBER	DESCRIPTION	QUANTITY
FortiNAC VM with HA	FNC-CAX-VM	FortiNAC Control and Application next-gen VM Server supports up to 50000 endpoint devices. Supporting VMware ESXi / ESX, Microsoft Hyper-V, Linux Kernel-based Virtual Machine (KVM), Nutanix and Cloud providers Amazon AWS, Microsoft Azure, Google GCP, Oracle OCI and Alibaba Cloud.	2
	FC-10-FNVXA-248-02-36	FortiCare Premium for FortiNAC VM, 3 years	2
8400 FortiNAC Base license with FortiCare for 36 months	LIC-FNAC-PLUS-1K	FortiNAC Perpetual PLUS License for 1K concurrent endpoint devices. Provides endpoint visibility and dynamic VLAN steering, advanced network access controls, and automated provisioning for users, guests, and devices	8
	LIC-FNAC-PLUS-100	FortiNAC Perpetual PLUS License for 100 concurrent endpoint devices. Provides endpoint visibility and dynamic VLAN steering, advanced network access controls, and automated provisioning for users, guests, and devices	4
	FC2-10-FNAC0-240-02-36	FortiCare Premium Support (100 Endpoints) for FortiNAC PLUS deployments with 3 years.	84



Bill of Material Exercises

Exercise 2

Opportunity: New business

Customer segment: Global bottle manufacturing, mid-sized

Feature needed: IoT visibility and control, 3rd party contractor access control, local management (Americas, EMEA, and APAC) with central reporting.

Infrastructure: FortiGate, FortiEDR, FortiClient EMS, and FortiSIEM. Timely alert notification and ultimately security automation. Want FortiNAC hardware with HA, running in their own DC in each region.

Number of devices: 2,000 across 4 regions

Terms: 3-years with next-day delivery RMA service on hardware appliance and 2-year for license terms.

Here is the proposed bill of material (BoM) using hardware appliance, with 3-year term and support:

	PART NUMBER	DESCRIPTION	QUANTITY
FortiNAC Manager Hardware Appliance with HA Cluster	FNC-M-550F	F series of the FortiNAC Manager hardware. Supports up to 100 CA's servers.	2
	FC-10-NF550-247-02-36	FortiCare Premium support for FNAC Manager, 3 years	2
	FC-10-NF550-210-02-36	Next-day delivery RMA service	2
FortiNAC CA Hardware Appliance with HA Cluster	FNC-CA-500F	F series of the FortiNAC CA hardware supporting up to 15000 endpoints.	8
	FC-10-NF500-247-02-36	FortiCare Premium support for FNAC CA-500F, 3 years	8
	FC-10-NF500-210-02-36	Next-day delivery RMA service	8
2000 FortiNAC Pro license with FortiCare for 36 months	FC3-10-FNAC1-209-01-36	FortiNAC Pro License Subscription, 500 endpoints	4

Exercise 3

Opportunity: Expansion

Customer segment: Transportation company

Locations: 700 stations

Feature needed: Already have device visibility and access control. Now need automated response and remediation to reduce manual processing.

Infrastructure: FortiNAC deployed with Plus license. Six regional data centers and two core data centers in HA mode and the control network services are distributed between the six regional data centers.

Number of devices: 13000 (2000 employees, 4500 connected IT devices and 7500 IoT devices, and up to 1000 guest devices)

Term: 1-year

The following BoM reflect the HA infrastructure in VM and added Plus license and support with 1-year term:

	PART NUMBER	DESCRIPTION	QUANTITY
HA cluster of FortiNAC Manager VM for the core data center with FortiCare for 12 months:	FNC-MX-VM	FortiNAC Manager next-gen VM Server supports up to 100 CA Servers. Supporting VMware ESXi / ESX, Microsoft Hyper-V, Linux Kernel-based Virtual Machine (KVM), Nutanix and Cloud providers Amazon AWS, Microsoft Azure, Google GCP, Oracle OCI and Alibaba Cloud.	2
	FC-10-FNVXM-248-02-12	FortiCare for FortiNAC Manager, VM, 1 year	2
HA clusters of FortiNAC CA VM for each regional data center with FortiCare for 12 months:	FNC-CAX-VM	FortiNAC Control and Application next-gen VM Server supports up to 50000 endpoint devices. Supporting VMware ESXi / ESX, Microsoft Hyper-V, Linux Kernel-based Virtual Machine (KVM), Nutanix and Cloud providers Amazon AWS, Microsoft Azure, Google GCP, Oracle OCI and Alibaba Cloud.	12
	FC-10-FNVXA-248-02-12	FortiCare Premium for FortiNAC VM, 1 year	12
13,000 FortiNAC Plus license	LIC-FNAC-PLUS-1K	FortiNAC Plus License, Perpetual, 1000 endpoints	3
	LIC-FNAC-PLUS-10K	FortiNAC Plus License, Perpetual, 10K endpoints	1
	FC2-10-FNAC0-240-02-12	FortiCare for Plus License, 100 end points, 1 year	130



Bill of Material Exercises

Exercise 4

Opportunity: Expansion

Customer segment: Retail company

Locations: 1700 stores nationwide

Features needed: Device and user visibility

Infrastructure: FortiGate SD-WAN. Deployed FortiNAC CA VM at one data center to manage 10 store locations as the first trial phase with roughly 1000 devices to support. Now, they are ready to expand the deployment into all 1700 stores. The customer wants to have the hardware-based offering with the HA cluster.

Number of devices: 170,000 devices

Term: 12 months

The customer needs perpetual license with 1-year term:

	PART NUMBER	DESCRIPTION	QUANTITY
HA cluster of FortiNAC Manager Hardware with FortiCare	FNC-M-550F	F series of the FortiNAC Manager hardware. Supports up to 100 CA's servers.	2
	FC-10-NF550-247-02-12	FortiCare Premium for FortiNAC Manager, VM, 1 year	2
	FC-10-NF550-210-02-12	Next-day delivery RMA service for 550F	2
HA clusters of FortiNAC CA 700F large deployment unit for up to 50 000 managed endpoints for each regional DC with FortiCare	FNC-CA-700F	F series of the FortiNAC CA hardware supporting up to 50000 endpoints, large deployment	14
	FC-10-NF700-247-02-12	FortiCare Premium for FortiNAC 700F, 1 year	14
	FC-10-NF700-210-02-12	Next-day delivery RMA service for 700F	14
170 000 FortiNAC Plus licenses with FortiCare	LIC-FNAC-PLUS-50K	FortiNAC Plus License, Perpetual, 50K endpoints	3
	LIC-FNAC-PLUS-10K	FortiNAC Plus License, Perpetual, 10K endpoints	2
	FC2-10-FNAC0-240-02-12	FortiCare for Plus License, 100 endpoints, 1 year	1700

Exercise 5

Opportunity: New business

Customer segment: Manufacturing

Locations: Factories in Latin America, HQ in Germany with a total of 221 remote sites distributed across the globe.

Features needed: Central managed hosted on EMEA Data-Centers, one pair of CA HA 1+1 per remove site (221), fully endpoint control and compliance for 100,000 devices, profiling and visibility for industrial network.

Infrastructure: Remote sites with FortiGate, FortiSwitch and FortiAP, for industrial environments they already have Fortinet rugged devices and want to make the integration with 3rd party platforms like Nozomi, Claroty and Armis.

Number of devices: 100,000

Term: PRO Perpetual licensing with 5 years of Forticare.

Here is the proposed bill of material (BoM) using VM, with five-year term and support:

	PART NUMBER	DESCRIPTION	QUANTITY
FortiNAC CA VM – 221 Sites HA 1+1 Mode	FNC-CAX-VM	FortiNAC Control and Application next-gen VM Server supports up to 50000 endpoint devices. Supporting VMware ESXi / ESX, Microsoft Hyper-V, Linux Kernel-based Virtual Machine (KVM), Nutanix and Cloud providers Amazon AWS, Microsoft Azure, Google GCP, Oracle OCI and Alibaba Cloud.	442
	FC-10-FNVXA-248-02-60	FortiCare Premium for FortiNAC VM, 5 years	442
100,000 Endpoint Licensing PRO level.	LIC-FNAC-PRO-50K	FortiNAC Perpetual PRO License for 50K concurrent endpoint devices. Pro license level provides the ultimate in visibility, control and response	2
	FC3-10-FNAC0-240-02-60	FortiCare Premium Support (100 Endpoints) for FortiNAC PLUS deployments with 3 years.	1,000
FortiNAC Manager VM – N+1 Setup 1 Master + 2 Workers + 1 Stand-by	FNC-MX-VM	FortiNAC Manager next-gen VM Server supports up to 100 CA Servers. Supporting VMware ESXi / ESX, Microsoft Hyper-V, Linux Kernel-based Virtual Machine (KVM), Nutanix and Cloud providers Amazon AWS, Microsoft Azure, Google GCP, Oracle OCI and Alibaba Cloud.	4
	FC-10-FNVXM-248-02-60	FortiCare Premium for FortiNAC Manager VM, 5 Years	4



New FortiNAC-F Series

Fortinet has introduced a new generation of FortiNAC F-Series of virtual and physical appliances that come with new features, such as the following:

- New FortiNAC-F operating system
- New internal database
- Cloud deployment enhancements
- More scalable and performance capabilities
- New UI workflows of policy creation for:
 - EasyConnect
 - Endpoint compliance
 - Network access policy
 - Authentication policy
 - Captive web portals
 - User host profiles

New FortiNAC-F Series

The SKUs for the next generation of FortiNAC F-Series and VMs are available for Control and Application and Manager. The customer can choose the new SKU schema as follows:

FORTINAC CONTROL AND APPLICATION			FORTINAC MANAGER	
	OLD	NEXT GENERATION	OLD	NEXT GENERATION
VM Server	FNC-CA-VM	FNC-CAX-VM	FNC-M-VM	FNC-MX-VM

FORTINAC HARDWARE APPLIANCES		
	OLD	NEXT GENERATION
HW Model	FortiNAC-CA-500C	FortiNAC-CA-500F
	FortiNAC-CA-600C	FortiNAC-CA-600F
	FortiNAC-CA-700C	FortiNAC-CA-700F
	FortiNAC-M-550C	FortiNAC-M-500F



Appliance Migration from CentOS to FortiNAC-F OS

New appliance migration tool released:

- [Single Appliance](#)
- [FortiNAC Manager Environments](#)
- [High Availability](#)

Migration FAQ 1: What is the process for migrating?

- Purchase/acquire the NAC-OS VM (FNC-CAX-VM or Manager FNC-MX-VM).
- On the CentOS VM, if FortiNAC is on 8.x, upgrade to 9.x to one of the following versions: 9.1.10, 9.2.8 or 9.4.4 or v7.2.3
- A tool shipped with v7.2.x to copy customer data from the v9 system into a file, which they need to store in a laptop.
- Customer must log in to FortiCare to transfer their entitlements, including licenses and FortiCare contracts, from the old VM to the new. They need serial numbers of both old and new VMs, plus other information that FortiCare requires.
- Customer then logs into the new NAC-OS VM, upgrade to 7.2.2, where they can use a tool to read the file generated in step 3 and push the data into the local FortiNAC system. Now the new FortiNAC-OS based VM will have all the license, contracts, plus the data to operate.

Migration FAQ 2: Does the conversion tool convert Manager and all PODs?

Yes, the conversion tool will cover the CA and Manager, but the migration process needs to be done one by one, starting with the PODs and then migrating the Manager last.

Migration FAQ 3: Does the migration process cover all exiting deployed FortiNAC configs?

- Does not cover customer with Subscription Licensing.
- Does not cover HW appliances. The migration tool to refresh the FortiNAC-F install in the C-series is under production.

Migration FAQ 4: If we have a customer that is still running the old two appliance solution, FNC-C-VM and FNC-A-VM or older (FNC-C-1000C and FNC-A-1000C, FNC-C-2000C and FNC-A-2000C), will the conversion tool have the ability to migrate them from two appliances to one new FNC-CAX-VM? If not, assuming we would sell PS time to do that type of conversion?

For the old Control or Application appliances, the original migration tool will not cover that migration. A new migration tool has been created to migrate a separate C appliance and A appliance to a single NAC-OS appliance.



Appliance Migration from CentOS to FortiNAC-F OS

Migration Table reference sheet:

FORTINAC CONTROL & APPLICATION			
C-SERIES		F-SERIES	
VIRTUAL MACHINES - CA TO CAX			
Product	SKU	Product	SKU
FortiNAC-CA-VM	FNC-CA-VM	FortiNAC-CAX-VM	FNC-CAX-VM
Appliance Maintenance Coverage	FC-10-NCVCA-248-02-xx	Next-gen Appliance Maintenance Coverage	FC-10-FNVXA-248-02-xx
VIRTUAL MACHINES - M TO MX			
FortiNAC-M-VM	FNC-M-VM	FortiNAC-MX-VM	FNC-MX-VM
Appliance Maintenance Coverage	FC-10-NCV0M-248-02-xx	Next-gen Appliance Maintenance Coverage	FC-10-FNVXM-248-02-xx
HARDWARE MACHINES - 500C TO 500F			
FortiNAC-CA-500	FNC-CA-500C	FortiNAC-CA-500F	FNC-CA-500F
Appliance Maintenance Coverage	FC-10-NC500-xx-xxxx	Next-gen Appliance Maintenance Coverage	FC-10-NF500-xx-xx-xx
HARDWARE MACHINES - 600C TO 600F			
FortiNAC-CA-600C	FNC-CA-600C	FortiNAC-CA-600F	FNC-CA-600F
Appliance Maintenance Coverage	FC-10-NC600-xx-xxxx	Next-gen Appliance Maintenance Coverage	FC-10-NF600-xx-xx-xx
HARDWARE MACHINES - 700C TO 700F			
FortiNAC-CA-700C	FNC-CA-700C	FortiNAC-CA-700F	FNC-CA-700F
Appliance Maintenance Coverage	FC-10-NC700-xx-xxxx	Next-gen Appliance Maintenance Coverage	FC-10-NF700-xx-xx-xx
HARDWARE MACHINES - 550C TO 550F			
FortiNAC-M-550C	FNC-M-550C	FortiNAC-M-550F	FNC-M-550F
Appliance Maintenance Coverage	FC-10-NC550-xx-xxxx	Next-gen Appliance Maintenance Coverage	FC-10-NF550-xx-xx-xx
LEGACY VIRTUAL MACHINES FORTINAC - C AND A TO CAX			
FortiNAC-C-VM	FNC-C-VM	FortiNAC-CAX-VM	FNC-CAX-VM
Appliance Maintenance Coverage	FC-10-NCV0C-248-02-xx	Next-gen Appliance Maintenance Coverage	FC-10-FNVXA-248-02-xx
FortiNAC-A-VM	FNC-A-VM		
Appliance Maintenance Coverage	FC-10-NCV0C-248-02-xx		
LEGACY PHYSICAL MACHINES FORTINAC - 1000 SERIES C AND A TO F-SERIES			
FortiNAC-C-1000C	FNC-C-1000C	FortiNAC-CA-500F	FNC-CA-500F
Appliance Maintenance Coverage	FC-10-NC1KC-247-02-xx	Next-gen Appliance Maintenance Coverage	FC-10-NF500-xx-xx-xx
FortiNAC-A-1000C	FNC-A-1000C		
LEGACY PHYSICAL MACHINES FORTINAC - 2000 SERIES C AND A TO F-SERIES			
FortiNAC-C-2000C	FNC-C-2000C	FortiNAC-CA-700F	FNC-CA-700F
Appliance Maintenance Coverage	FC-10-NC2KC-247-02-xx	Next-gen Appliance Maintenance Coverage	FC-10-NF700-xx-xx-xx
FortiNAC-A-2000C	FNC-A-2000C		



www.fortinet.com

Copyright © 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

PROPOSTA TÉCNICA

DO OBJETO: O objeto do presente contrato é aquisição de ativos de rede e Solução de NAC, sob a forma de entrega parcelada, conforme condições do Termo de Referência.

O prazo de vigência da contratação é de 12 (doze) meses contados da publicação do contrato no Portal Nacional de Contratações Públicas - PNCP, na forma do art. 105 da Lei nº 14.133, de 2021.

PROJETO AGE - ADESÃO ARP DPE-PA					
LOTE	ITEM	DESCRIÇÃO	QTDE	VALOR VENDA UNITÁRIO	VALOR VENDA TOTAL
1	1	FORTINAC - 1000 DISPOSITIVOS SIMULTANEOS	1	R\$ 595.138,64	R\$ 595.138,64
1	2	FORTINAC - ADD ON	6	R\$ 107.819,03	R\$ 646.914,17
VALOR TOTAL					R\$ 1.242.052,81

Detalhamento Técnica:

LOTE 2 - Item 1 – Licenciamento para 1000 dispositivos simultâneos. (licenciamento perpétuo)

- 2 x FNC-CAX-VM - LICENÇA DE SOFTWARE - CONTROLE E APLICATIVO FORTINAC SERVIDOR VM DE PROXIMA GERAÇÃO VMWAREHYPERVAWSAZUREKVM.
- 2 x FC-10-FNVXA-248-02-60 SERVIÇO - FORTINAC CONTROL AND APPLICATION EXTENDED-VM 5 YEAR FORTICARE PREMIUM SUPPORT
- 10 x FC3-10-FNAC0-240-02-60 - SERVIÇO - FORTICARE SUPPORT FOR FORTINAC LICENSE 5 YEAR 24X7 FORTICARE CONTRACT (100 ENDPOINTS) FOR FORTINAC PRO DEPLOYMENTS.
- 1 x LIC-FNAC-PRO-1K - LICENÇA DE SOFTWARE LICENÇA FORTINAC PRO PARA 1K DISPOSITIVOS ENDPOINT SIMULTANEOS. O NIVEL DE LICENÇA PRO FORNECE O MAXIMO EM VISIBILIDADE, CONTROLE E RESPOSTA
- Contido serviço de suporte do fabricante durante o período de garantia.

LOTE 2 - Item 2 – Add-on de 500 dispositivos simultâneos. (licenciamento perpétuo)

- 30 x LIC-FNAC-PRO-100 LICENÇA DE SOFTWARE - FORTINAC PRO LICENSE FOR 100 CONCURRENT ENDPOINT DEVICES. PRO LICENSE LEVEL PROVIDES THE ULTIMATE IN VISIBILITY, CONTROL AND RESPONSE
- 30 x FC3-10-FNAC0-240-02-60 - LICENÇA DE SOFTWARE FORTINAC PRO LICENSE FOR 100 CONCURRENT ENDPOINT DEVICES. PRO LICENSE LEVEL PROVIDES THE ULTIMATE IN VISIBILITY, CONTROL AND RESPONSE
- Contido serviço de suporte do fabricante durante o período de garantia.

Serviços de Instalação:

- Serviço de Instalação e suporte conforme termo de referência.

Brasília, 27 de abril 2026.



Murilo Rossetto

Representante Legal

CPF:036.031.821-54

Cargo na empresa: Diretor Comercial

AllTech Soluções em Tecnologia Ltda