Cisco Virtual Network Management Center GUI Configuration Guide, Release 1.3

First Published: January 31, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-25827-01

CONTENTS

Preface

This preface includes the following sections:

Audience

This guide is intended primarily for data center administrators with responsibilities and expertise in one or more of the following:

- Server administration
- Storage administration
- Network administration
- Network security

Organization

This document includes the following chapters:

Chapter	Title	Description
Chapter 1	Overview	Contains an overview of the Cisco VNMC.
Chapter 2	VNMC GUI Overview	Contains an overview of the Cisco VNMC GUI.

Chapter	Title	Description
Chapter 3	Configuring Primary Authentication	Describes how to configure LDAP providers and selecting a primary authentication service.
Chapter 4	Configuring Role-Based Access Control	Describes how to configure role-based access control including user locales, user roles, locally authenticated user accounts and monitoring user sessions.
Chapter 5	Configuring Trusted Points	Describes how to configure trusted points.
Chapter 6	Configuring VNMC Profiles	Describes how to configure policies in the VNMC profile and a default profile.
Chapter 7	Configuring VM Managers	Describes how to configure VM Managers.
Chapter 8	Configuring Tenants	Describes how to configure tenants, data centers, applications, and tiers.
Chapter 9	Configuring Security Policies	Describes how to configure firewall policies, security profiles, and security profile dictionary.
Chapter 10	Configuring Device Policies	Describes how to configure device policies and device profiles.
Chapter 11	Configuring Managed Resources	Describes how to configure managed resources including compute firewall and pool.
Chapter 12	Configuring Backups	Describes how to configure backup operations, import operations, and import operations.

Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands, keywords, GUI elements, and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.

Convention	Indication
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier` font	Terminal sessions and information that the system displays appear in `courier` font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*.

Tip Means *the following information will help you solve a problem*.

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning Means *reader be warned*. In this situation, you might perform an action that could result in bodily injury.

Related Documentation

Cisco Virtual Network Management Center

The following Cisco Virtual Network Management Center documents are available on Cisco.com at the following url:

http://www.cisco.com/en/US/products/ps11213/tsd_products_support_series_home.html

- *Release Notes for Cisco Virtual Network Management Center, Release 1.3*
- *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(3.1) and Cisco Virtual Network Management Center, Release 1.3 Installation and Upgrade Guide*
- *Cisco Virtual Network Management Center CLI Configuration Guide, Release 1.3*
- *Cisco Virtual Network Management Center GUI Configuration Guide, Release 1.3*
- *Cisco Virtual Network Management Center XML API Reference Guide, Release 1.3*

Cisco Virtual Security Gateway for Nexus 1000V Series switch

The following Cisco Virtual Security Gateway for Nexus 1000V Series switch documents are available on Cisco.com at the following url:

http://www.cisco.com/en/US/products/ps11208/tsd_products_support_model_home.html

- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Release Notes, Release 4.2(1)VSG1(3.1)*
- *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(3.1) and Cisco Virtual Network Management Center, Release 1.3 Installation and Upgrade Guide*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch License Configuration Guide, Release 4.2(1)VSG1(3.1)*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Configuration Guide, Release 4.2(1)VSG1(3.1)*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Command Reference, Release 4.2(1)VSG1(3.1)*
- *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Troubleshooting Guide, Release 4.2(1)VSG1(3.1)*

Cisco Nexus 1000V Series switch

The Cisco Nexus 1000V Series switch documents are available on Cisco.com at the following url: http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to vnmc-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

Overview

This chapter includes the following sections:

Cisco Virtual Network Management Center Overview

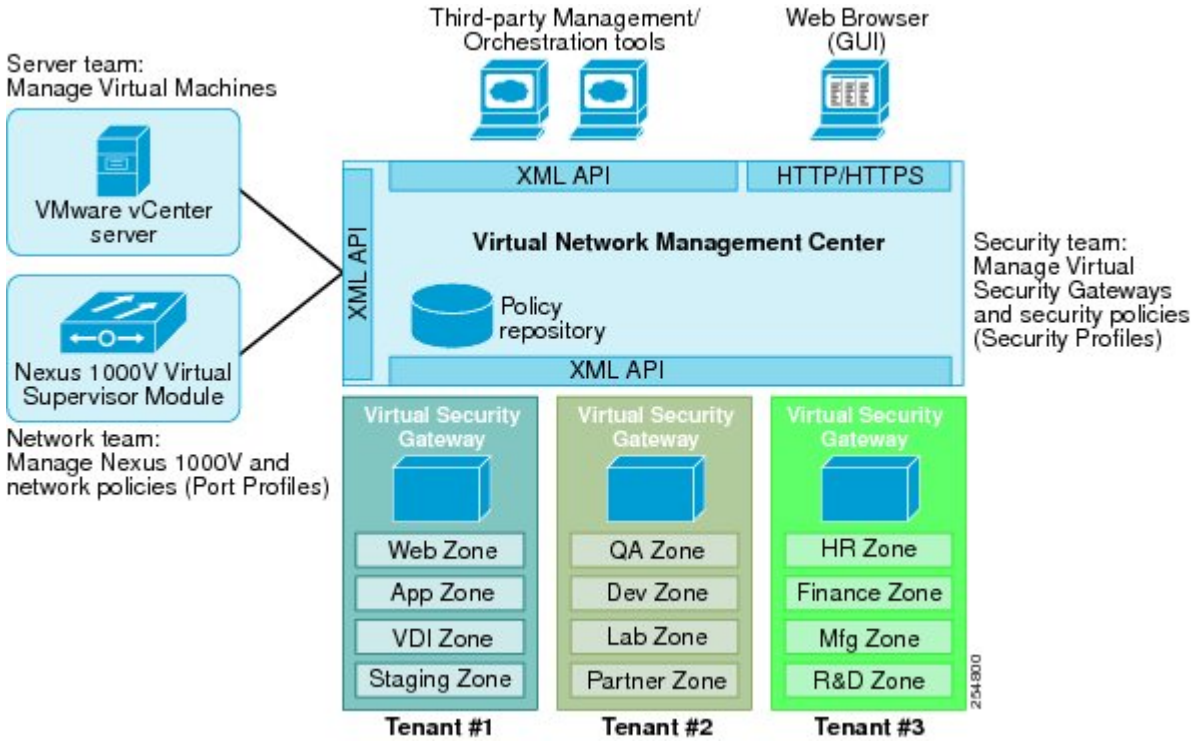
Cisco Virtual Network Management Center (Cisco VNMC) is a virtual appliance, based on Red Hat Enterprise Linux, that provides centralized device and security policy management of Cisco Virtual Security Gateways (Cisco VSGs) for the Cisco Nexus 1000V Series switch. Designed for multi-tenant operation, the Cisco VNMC provides seamless, scalable, and automation-centric management for virtualized data center and cloud environments. With built-in GUI, CLI, and XML APIs, the Cisco VNMC allows you to manage Cisco VSGs that are deployed throughout the data center from a centralized location. The Cisco VNMC is built on the information model-driven architecture where each managed device is represented by its sub-components (or objects) that are parametrically defined. This model-centric approach enables the Cisco VNMC to provide secure multi-tenant virtualized infrastructure with Cisco VSGs.

The Cisco VNMC provides the following key benefits:

- Rapid and scalable deployment through policy management based on security profiles
- Seamless operational management through XML APIs that enable programmatic integration with third-party management and orchestration tools

- Non-disruptive administration model enabling greater collaboration across security and server teams while maintaining administrative separation and reducing administrative errors

Figure 1: Cisco VNMC in a Multi-Tenant Environment



Cisco VNMC provides centralized device and policy management of Cisco VSGs in a multi-tenant virtual data center and/or private/public cloud.

The Cisco VNMC uses security profiles for tenant-centric configuration of security policies. A security profile is a collection of security policies that can be pre-defined and applied on an on-demand basis at the time of VM instantiation. This profile-driven approach significantly simplifies authoring, deployment, and management of security policies in a dense multi-tenant environment while also enhancing deployment agility and scale. Security profiles also help reduce administrative errors as well as simplify audits.

An important characteristic of Cisco VNMC is its north-bound XML API support, which facilitates coordination with third-party provisioning tools for programmatic provisioning and management of Cisco VSGs.

By providing visual and programmatic controls, the Cisco VNMC enables the security operations team to author and manage security policies for virtualized infrastructure, while enhancing collaboration with server and network operations teams. This non-disruptive administration model ensures that administrative segregation of duties remain in place to minimize administrative errors as well as to simplify compliance and audit requirements. The Cisco VNMC operates with the Nexus 1000V Virtual Supervisor Module (VSM) to achieve the following workflow:

- The network administrator can author and manage port profiles through Cisco Nexus 1000V distribute virtual switches. Port profiles on the Cisco Nexus 1000V Series switch can be propagated to the VMware Virtual Center as port groups and referenced by Virtual Machines.

- Security profiles are created in the Cisco VNMC and referenced in Cisco Nexus 1000V Series switch port profiles. Port profiles are created on the Nexus 1000V VSM.
- The server administrator can select the appropriate port profile in the VMware Virtual Center when instantiating a virtual machine.

The Cisco VNMC implements an information-model driven architecture in which each managed device, such as the Cisco VSG, is represented by the object information model of the device. Specifically, this model-driven architecture includes:

- A centralized repository for managing security policies and object configurations, thus allowing the managed devices to be stateless
- A centralized resource management function that distinctly manages pool of devices that are commissioned in service and pool of devices that are available for commissioning. This simplifies large-scale deployments because managed devices can be pre-instantiated and then configured on demand and devices can be allocated and de-allocated dynamically across commissioned and non-commissioned pools
- A distributed management-plane function implemented using an embedded management agent on each managed device, thus enabling a scalable management framework

Cisco VNMC System Requirements

Cisco VNMC has the following system requirements:

- Cisco VNMC Virtual Appliance—1 virtual CPU at 1.5-GHz, 2-GB RAM, 25-Gb hard disk (vDisk), 1 management network interface

Note 3-GB RAM is required for a Cisco VNMC ISO installation.

- Hypervisor and Hypervisor Manager—
  - VMware vSphere 4.1.0 and 5.0 releases with VMware ESX or ESXi
  - VMware vCenter 4.1.0 and 5.0 releases
- Interfaces and Protocols—HTTP/HTTPS, Lightweight Directory Access Protocol (LDAP)
- Web-based GUI client—
  - Flash 10.1
  - Operating system—Support details are as follows:

Table 1: Operating System Support Matrix

Operating System	Internet Explorer 7.x and 8.x	Firefox 8.x
Windows	Supported	Supported
Apple MAC OS	X	X

Operating System	Internet Explorer 7.x and 8.x	Firefox 8.x
Linux	X	X

Note You can find VMware compatibility guides at http://www.vmware.com/resources/compatibility/search.php

Cisco VNMC Features

The Cisco VNMC includes the following features:

Multi-device Management

All Cisco Virtual Security Gateway for Nexus 1000V Series Switch devices are centrally managed which simplifies provisioning and troubleshooting in a scaled-out data center. In addition, the device profile object specifies device configuration policies that you can apply to one or more firewall profile managed resources.

Security Profile

A security profile enables you to represent the Cisco VSG security policy configuration in a profile, which simplifies provisioning, reduces administrative errors during security policy changes, reduces audit complexities, and enables a highly scaled out data center environment.

Stateless Device Provisioning

The stateless configuration model is enabled with a management agent that is embedded with Cisco VSGs, that allows the Cisco VNMC to be a highly scalable device provisioning model.

Security Policy Management

Security policies are authored, edited, and provisioned for all Cisco VSGs in a data center, which simplifies the operation and management of security policies as well as ensures that the required security is accurately represented in the associated security policies.

Context Aware Security Policies

The Cisco VNMC interacts with VMware vCenter to obtain VM contexts that you can leverage to institute granular policy controls across their virtual infrastructure.

Dynamic Security Policy and Zone Provisioning

The Cisco VNMC interacts with the Nexus 1000V VSM to bind the security profile with the corresponding Cisco Nexus 1000V Series switch port profile. When VMs are dynamically instantiated and applied to appropriate port profiles, their association to trust zones is also established.

Multi-tenant Management

The Cisco VNMC can manage Cisco VSGs and security policies in a dense multi-tenant environment, so that you can rapidly add or delete tenants and update tenant-specific configurations and security policies. This feature significantly reduces administrative errors, ensures segregation of duties within the administrative team, and simplifies audit procedures.

Role-Based Access Control

Role-Based Access Control (RBAC) simplifies operational tasks across different types of administrators, while allowing subject-matter experts to continue with their normal procedures. With RBAC, organizations are able to reduce administrative errors and simultaneously simplify auditing requirements. The Cisco VNMC supports local and remote authentication with RBAC.

XML-Based API

The Cisco VNMC full-featured XML APIs allow external system management and orchestration tools to programmatically provision Cisco VSGs and provide seamless and scalable operational management.

CHAPTER 2

Cisco VNMC GUI Overview

This chapter includes the following sections:

Overview of Cisco VNMC GUI

The Cisco VNMC GUI is web based and provides a GUI interface to the Cisco VNMC.

The Cisco VNMC GUI allows a user to configure the managed end-points, administrative operational tasks, and define various policies and artifacts. Administrators using the GUI component of the Cisco VNMC platform can manage and provision Cisco VSGs.

You can start and access the Cisco VNMC GUI from a computer that meets the following requirements:

- ***Table 2: Operating System Support Matrix***

Operating System	Internet Explorer 7.x and 8.x	Firefox 8.x
Windows	Supported	Supported
Apple MAC OS	X	X
Linux	X	X

- Adobe Flash Player 10.1

Note The title bar displays the name of the Cisco VNMC instance to which you are connected.

Logging in to Cisco VNMC GUI through HTTPS

The default HTTPS web link for Cisco VNMC GUI is `https://VNMC_IP_address`, where *VNMC_IP_address* represents the IP address assigned to Cisco VNMC. The IP address is the address for the management port.

Tip If you login using HTTP, you are automatically redirected to the HTTPS link.

Procedure

Step 1 In your web browser, type the Cisco VNMC web link or select the bookmark in your browser.

Step 2 In the Cisco VNMC page **Username** and **Password** fields, enter your username and password.

Step 3 Click **Login**.

Cisco VNMC Protected by a Firewall and Permitted Ports

For the Cisco VNMC GUI to work when Cisco VNMC is protected by a firewall, the following ports must be permitted to communicate with Cisco VNMC:

- Ports 443 (HTTP)
- 80 (HTTP/TCP)
- 843 (TCP)

Setting the Inactivity Timeout

You use the **Preferences** dialog box to set the inactivity timeout.

Procedure

Step 1 On the toolbar, click the **Preferences** link.

Step 2 In the **Preferences** dialog box, **Idle Timeout** field, set the number of minutes.
The range is from 5 to 60 minutes.

Step 3 Click **Apply**.

Logging Off Cisco VNMC GUI

Procedure

In Cisco VNMC GUI, click **Log Out** in the Toolbar.

Navigation Pane

The **Navigation** pane displays on the left side of the Cisco VNMC GUI below the title bar. This pane provides centralized navigation to all equipment and components in the Cisco VNMC instance. When you select a component in the **Navigation** pane, the object displays in the **Work** area. The **Navigation** pane has four tabs.

Tenant Management Tab

This tab contains a basic inventory of tenants in the Cisco VNMC instance. A system or server administrator can use this tab to create typed organizational hierarchies and enable multi-tenancy management domains. The typed organizational hierarchies are Tenant > Virtual Data Center > Application > Tier.

Resource Management Tab

This tab contains the components required to manage the logical resource pools such as Cisco VSGs, VSMs, and vCenters.

The subtabs below the **Resource Management** tab are the following:

- **Managed Resources**
- **Resources**
- **Capabilities**
- **Diagnostics**

Policy Management Tab

This tab contains the components to configure security policies and device profiles, and assign policies to those device profiles.

The subtabs below the **Policy Management** tab are the following:

- **Security Policies**
- **Device Configurations**
- **Capabilities**
- **Diagnostics**

Administration Tab

This tab contains the components to administer Cisco VNMC.

The subtabs below the **Administration** tab are the following:

- **Access Control**
- **Service Registry**
- **VNMC Profile**
- **VM Managers**
- **Diagnostics**
- **Operations**

Toolbar

The toolbar displays on the right side of the Cisco VNMC GUI above the **Work** pane. You can use the menu buttons in the toolbar to perform common actions, including the following actions:

- View your username in the Cisco VNMC instance
- Set your preferences for inactivity timeout from the Cisco VNMC
- Log out of the Cisco VNMC GUI
- View version details about the Cisco VNMC GUI
- Access online help for the Cisco VNMC GUI

Work Pane

The **Work** pane displays on the right side of the Cisco VNMC GUI. This pane displays details about the component selected in the **Navigation** pane.

The **Work** pane includes the following elements:

- A navigation bar that displays the path from the main node of the tab in the **Navigation** pane to the selected element. You can click any component in this path to display that component in the **Work** pane.
- A content area that displays tabs with information related to the component selected in the **Navigation** pane. The tabs displayed in the content area depend upon the selected component. You can use these tabs to view information about the component, create components, modify properties of the component, and examine a selected object.

CHAPTER 3

Configuring Primary Authentication

This chapter includes the following sections:

Primary Authentication

Cisco VNMC supports two methods to authenticate user logins:

- Local to Cisco VNMC
- Remote through LDAP

The role and locale assignment for a local user can be changed on Cisco VNMC. The role and locale assignment for a remote user can be changed on LDAP. If any of the following information related to a user is modified, the administrator must delete all the existing sessions of that user so that the new privileges take effect:

- the assigned role for a user
- the assigned locale for a user
- the privilege for a role that is assigned to a user
- the organization in a locale that is assigned to a user

Remote Authentication Providers

If a system is configured for the supported remote authentication services, you must create a provider for that service to ensure that Cisco VNMC can communicate with it.

User Accounts in Remote Authentication Services

You can create user accounts in Cisco VNMC or in the remote authentication server.

The temporary sessions for users who log in through remote authentication services can be viewed through the Cisco VNMC GUI.

User Roles and Locales in Remote Authentication Services

If you create user accounts in the remote authentication server, you must ensure that the accounts include the roles and locales those users require for working in Cisco VNMC and that the names of those roles and locales match the names used in Cisco VNMC. If an account does not have the required roles and locales, the user is granted only read-only privileges.

LDAP Attribute for User

In Cisco VNMC, the LDAP attribute that holds the LDAP user roles and locales are preset. This property is always a name-value pair. For example, by default CiscoAvPair specifies the role and locale information for the user and if the filter is specified, the LDAP search is restricted to those values that match the defined filter. By default, the filter is sAMAccountName=$userid. The user can change these values to match the setting on the LDAP server. When a user logs in, Cisco VNMC checks for the value of the attribute when it queries the remote authentication service and validates the user. The value should be identical to the username.

An example of LDAP property settings is as follows:

- **Timeout**—30
- **Retries**—1
- **Attribute**—CiscoAvPair
- **Filter**—sAMAccountName=$userid
- **Base DN**—DC=cisco, DC=com (The specific location in the LDAP hierarchy where Cisco VNMC will start the query for the LDAP user.)

Creating an LDAP Provider

Before You Begin

Configure users with the attribute that holds the user role and locale information for Cisco VNMC. You can use an existing LDAP attribute that is mapped to the Cisco VNMC user roles and locales or create a custom attribute, such as the CiscoAVPair attribute, which has an attribute ID of 1.3.6.1.4.1.9.287247.1. When you add the LDAP user to the LDAP server, specify the role and locale in the attribute (for example, shell:roles=network,aaa shell:locale=sanjose,dallas)

Configure the properties for the LDAP provider connections in Cisco VNMC.

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.

Step 2 In the **Navigation** pane, click the **Access Control** subtab.

Step 3 In the **Navigation** pane, select the **LDAP** node.

Step 4 In the **Work** pane, click the **Create LDAP Provider** link.

Step 5 In the **Create LDAP Provider** dialog box, complete the following fields :

Name	Description
Hostname/IP Address field	The hostname or IP address of the LDAP provider. If SSL is enabled, this field must match a Common Name (CN) in the security certificate of the LDAP database. **Note** If you use a hostname rather than an IP address, you must configure a DNS server in the Cisco VNMC server.
Key field	The password for the LDAP database account specified in the **Root DN** field. The maximum is 32 characters.
Root DN field	The Distinguished Name (DN) for an LDAP database account that has read and search permissions for all objects under the base DN. The maximum supported string length is 128 characters.
Port field	The port through which Cisco VNMC communicates with the LDAP database. The standard port number is 389.
Enable SSL check box	The check box to enable SSL.

Note Depending upon the object you select in the table, different options will appear in the area above the table.

Step 6 Click **OK**.

Step 7 In the **Work** pane, click **Save**.

Following is an example of creating an LDAP provider:

- **Hostname/IP Address**—Provider-blr-sam-aaa-10.cisco.com
- **Key**—xxxxxx (The password of the LDAP database account specified in the **Root DN** field.)

- **Root DN**— CN=bob,DC=cisco,DC=com (The value of CN is the name of a user with query privileges. DC refers to the location in the LDAP directory where a user is created.)
- **Port**—389
- **Enable SSL**—check box

What to Do Next

Select LDAP as the primary authentication service. For more information, see Selecting a Primary Authentication Service, on page 15.

Editing an LDAP Provider

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.

Step 2 In the **Navigation** pane, click the **Access Control** subtab.

Step 3 In the **Navigation** pane, select the **LDAP** node.

Step 4 In the **Work** pane, click on an *LDAP Provider_name*.

Step 5 Click the **Edit** link.

Step 6 In the **Edit** dialog box modify the appropriate fields with the information about the LDAP service you want to use:

Name	Description
Name field	The hostname or IP address on which the LDAP provider resides. If SSL is enabled, this field must exactly match a Common Name (CN) in the security certificate of the LDAP database. If you use a hostname rather than an IP address, you must configure a DNS server in the Cisco VNMC This field is not editable.
Key field	The password for the LDAP database account specified in the **Root DN** field.
Root DN field	The distinguished name (DN) for the LDAP database account. This account has read and search permissions for all objects under the base DN. Password length maximum is 128 characters.
Port field	The port through which Cisco VNMC communicates with the LDAP database. The standard LDAP database port number is 389.

Name	Description
Enable SSL check box	The check box that you check to enable Secure Socket Layer (SSL).

Step 7 Click **OK**.

Step 8 In the **Work** pane, click **Save**.

Deleting an LDAP Provider

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.

Step 2 In the **Navigation** pane, click the **Access Control** subtab.

Step 3 In the **Navigation** pane, click **LDAP**.

Step 4 In the **Work** pane, click the *LDAP provider_name* that you want to delete.

Step 5 Click the **Delete** link.

Step 6 In the **Confirm** dialog box, click **Yes**.

Step 7 In the **Work** pane, click **Save**.

Selecting a Primary Authentication Service

Note If the default authentication is set to LDAP, and the LDAP servers are not operating or unreachable, the local admin user can login any time and make changes to the AAA system.

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.

Step 2 In the **Navigation** pane, click the **Access Control** subtab.

Step 3 In the **Navigation** pane click the **Authentication** node.

Step 4 In the **Work** pane, click the **Properties** tab.

Step 5 On the **Properties** tab, complete the following fields:

Name	Description
Default Authentication drop-down list	The default method by which a user is authenticated during remote login. This can be one of the following methods: • **ldap**—The user must be defined on the LDAP server specified for this Cisco VNMC instance. • **local**—The user must be defined locally in this Cisco VNMC instance. • **none**—A password is not required when the user logs in remotely.
Role Policy to Remote Users drop-down list	The action taken when a user attempts to log in and the LDAP server does not supply a user role with the authentication information. This can be one of the following actions: • **assign-default-role**—The user is allowed to log in with a read-only user role. • **no-login**—The user is not allowed to log into the system, even if the user name and password are correct.

Step 6 Click **Save**.

CHAPTER 4

Configuring Role-Based Access Control

This chapter includes the following sections:

Role-Based Access Control

Role-Based Access Control (RBAC) is a method of restricting or authorizing system access for users based on user roles and locales. A role defines the privileges of a user in the system and the locale defines the organizations (domains) that a user is allowed access. Because users are not directly assigned privileges, management of individual user privileges is simply a matter of assigning the appropriate roles and locales.

A user is granted write access to desired system resources only if the assigned role grants the access privileges and the assigned locale allows access. For example, a user with the Server Administrator role in the Engineering organization could update server configurations in the Engineering organization but could not update server configurations in the Finance organization unless the locales assigned to the user include the Finance organization.

User Accounts for Cisco VNMC

User accounts are used to access the system. Up to 48 local user accounts can be configured in each Cisco VNMC instance. Each user account must have a unique username.

A local user can be authenticated using a password or an SSH public key. The public key can be set in either of the two formats: OpenSSH and SECSH.

Default User Account

Each Cisco VNMC instance has a default user account, admin, which cannot be modified or deleted. This account is the system administrator or superuser account and has full privileges. There is no default password assigned to the admin account; you must choose the password during the initial system setup.

Expiration of User Accounts

User accounts can be configured to expire at a predefined time. When the expiration time is reached the user account is disabled.

By default, user accounts do not expire.

Guidelines for Cisco VNMC Usernames

The username is also used as the login ID for Cisco VNMC. When you assign usernames to Cisco VNMC user accounts, consider the following guidelines and restrictions:

- The login ID can contain between 1 and 32 characters, including the following:
  - Any alphabetic character
  - Any digit
  - . (period)
  - _ (underscore)
  - - (dash)
  - @
- The unique username for each user account cannot be all-numeric. You cannot create a local user with an all-numeric username.
- The unique username cannot start with a number.
- If an all-numeric username exists on an AAA server (LDAP) and is entered during login, Cisco VNMC cannot log in the user.

After you create a user account, you cannot change the username. You must delete the user account and create a new one.

Note You can create up to 48 user accounts in a Cisco VNMC instance.

Guidelines for Cisco VNMC Passwords

For authentication purposes, a password is required for each user account. To prevent users from choosing insecure passwords, each password must be strong. If the **Password Strength Check** is enabled, then Cisco VNMC rejects any password that does not meet the following requirements:

- Must contain a minimum of 8 characters.
- Must contain at least three of the following:
  - Lower case letters
  - Upper case letters
  - Digits
  - Special characters
- Must not contain a character that is repeated more than 3 times consecutively, such as aaabbb.
- Must not be identical to the username or the reverse of the username.
- Must pass a password dictionary check. For example, the password must not be based on a standard dictionary word.
- Must not contain the following symbols: $ (dollar sign), ? (question mark), and = (equals sign).
- Should not be blank for local user and admin accounts.

Note The **Password Strength Check** is enabled by default. You can disable it from the **Locally Authenticated Users** Pane.

Note If the Cisco VNMC instance is configured to use remote authentication with LDAP, passwords for those remote accounts can be blank. With this configuration, the remote credentials store is used just for authentication, not authorization. The definition of the local user role definition applies to the remotely authenticated user.

User Roles

User roles contain one or more privileges that define the operations allowed for the user who is assigned the role. A user can be assigned one or more roles. A user assigned multiple roles has the combined privileges of all assigned roles. For example, if Role1 has policy-related privileges, and Role2 has tenant-related privileges, users who are assigned to both Role1 and Role2 have policy and tenant related privileges.

All roles include read access to all configuration settings in the Cisco VNMC instance. The difference between the read-only role and other roles is that a user who is only assigned the read-only role cannot modify the system state. A user assigned another role can modify the system state in that user's assigned area or areas.

The system contains the following default user roles:

aaa

User has read and write access to users, roles, and AAA configuration. Read access to the rest of the system.

admin

User has complete read-and-write access to the entire system and has all privileges. The default admin account is assigned this role by default, and it cannot be changed.

network

User creates organizations, security policies, and device profiles.

operations

User acknowledges faults and performs some basic operations such as logging configuration.

read-only

User has read-only access to system configuration and operational status with no privileges to perform any operations.

Roles can be created, modified to add new or remove existing privileges, or deleted. When a role is modified, the new privileges are applied to all users assigned to that role. Privilege assignment is not restricted to the privileges defined for the default roles. That is, you can use a custom set of privileges to create a unique role. For example, the default Network and Operations roles have different sets of privileges, but a new Network and Operations role can be created that combines the privileges of both roles.

If a role is deleted after it has been assigned to users, it is also deleted from those user accounts.

The role and locale assignment for a local user can be changed on Cisco VNMC. The role and locale assignment for a remote user can be changed on LDAP. If any of the following information related to a user is modified, the administrator must delete all the existing sessions of that user so that the new privileges take effect:

- the assigned role for a user
- the assigned locale for a user
- the privilege for a role that is assigned to a user
- the organization in a locale that is assigned to a user

Privileges

User Privileges

Privileges give users assigned to user roles access to specific system resources and permission to perform specific tasks. The following table lists each privilege and its description.

Privilege Name	Description
AAA	System security and AAA
Admin	System administration

Privilege Name	Description
read-only	Read-only access Read-only cannot be selected as a privilege; it is assigned to every user role
Resource Configuration	Compute firewall configuration
Policy Management	Compute firewall policy
Fault Management	Alarms and alarm policies
Operations	Logs, core file management, and **show tech-support** command
Tenant Management	Create, delete, and modify tenants and organization containers

Privileges and Role Assignments

The following table lists the out-of-box default role name for each privilege.

Default Role Name	Privilege Name
aaa	aaa
admin	admin
network	policy, res-config, tenant
operations	fault, operations
read-only	read-only

User Locales

A user can be assigned one or more locales. Each locale defines one or more organizations (domains) to which the user is allowed access. In addition, the user has read-only access privileges outside their assigned locale and going up the organization tree. This enables the user to use these objects when creating policies. One exception to this rule is a locale without any organizations, which gives unrestricted access to system resources in all organizations. Only the objects under organizations are controlled by locales. Access to other objects such as users, roles, and resources that are not present in the organization tree are not affected by locales.

Users with AAA Administrator privileges (AAA Administrator role) can assign organizations to the locale of other users. The assignment of organizations is restricted to only those in the locale of the user assigning the organizations. For example, if a locale contains only the Engineering organization then a user assigned that locale can only assign the Engineering organization to other users.

Attention AAA privileges must be carefully assigned because it allows a user to manage users' privileges and role assignments.

You can hierarchically manage organizations. A user that is assigned at a top level organization has automatic access to all organizations under it. For example, an Engineering organization can contain a Software Engineering organization and a Hardware Engineering organization. A locale containing only the Software Engineering organization has access to system resources only within that organization; however, a locale that contains the Engineering organization has access to the resources for both the Software Engineering and Hardware Engineering organizations.

The role and locale assignment for a local user can be changed on Cisco VNMC. The role and locale assignment for a remote user can be changed on LDAP. If any of the following information related to a user is modified, the administrator must delete all the existing sessions of that user so that the new privileges take effect:

- the assigned role for a user
- the assigned locale for a user
- the privilege for a role that is assigned to a user
- the organization in a locale that is assigned to a user

Configuring User Roles

Creating a User Role

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.

Step 2 In the **Navigation** pane, click the **Access Control** subtab.

Step 3 In the **Navigation** pane click **Roles**.

Step 4 In the **Work** pane, click **Create Role**.

Step 5 In the **Create Role** dialog box, complete the following fields:

Name	Description
Name field	The name of the user role.

Name	Description
Privileges list	A lists of roles. To assign a privilege to the selected user, check one or more of the following check boxes: • **Admin** • **AAA** • **Fault Management** • **Operations** • **Policy Management** • **Resource Configuration** • **Tenant Management** **Note** You can assign the **admin** privilege, which includes all the privileges, or you can assign other privileges.

Step 6 Click **OK**.

Editing a User Role

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **Access Control** subtab.
Step 3 In the **Navigation** pane, click the **Roles** node.
Step 4 In the **Work** pane, select the *Role_name* you want to edit
Step 5 Click the **Edit** link.
Step 6 In the **Edit** dialog box, check or uncheck the boxes for the privileges you want to add to the role.
Step 7 Click **OK**.

Deleting a User Role

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **Access Control** subtab.
Step 3 In the **Navigation** pane, click the **Roles** node.
Step 4 In the **Work** pane, click the user role you want to delete.
Step 5 Click the **Delete** link.
Step 6 In the **Confirm** dialog box, click **Yes**.

Configuring User Locales

Creating a Locale

Before You Begin

One or more organizations must exist before you create a locale.

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **Access Control** subtab.
Step 3 In the **Navigation** pane, click the **Locales** node.
Step 4 In the **Work** pane click the **Create Locale** link.
Step 5 In the **Create Locale** dialog box, complete the following fields:

Table 3: Properties Area

Name	Description
Name field	The name for the locale. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.

Name	Description
Description list	The description of the locale. This name can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.

Step 6 Click **OK**.

What to Do Next

Add the locale to one or more user accounts. For more information, see Changing the Locales Assigned to a Locally Authenticated User Account, on page 30.

Editing a Locale

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **Access Control** subtab.
Step 3 In the **Navigation** pane, click the **Locales** node.
Step 4 In the **Work** pane, click the locale you want to edit.
Step 5 Click the **Edit** link.
Step 6 In the **Description** field, change the description as appropriate.
Step 7 Click the **Assign Organizations** link and do the following:
a) Expand the **root** node to view the organizations in the Cisco VNMC instance.
b) Check the appropriate check boxes.
Step 8 Click **OK**.

Deleting a Locale

Before You Begin

Caution If the locale you want to delete is assigned to any user/s, remove the locale from the user list of locales.

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **Access Control** subtab.
Step 3 In the **Navigation** pane, click the **Locales** node.
Step 4 In the **Work** pane, click the locale you want to delete.
Step 5 Click the **Delete** link.
Step 6 In the **Confirm** dialog box, click **Yes**.

Assigning an Organization to a Locale

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **Access Control** subtab.
Step 3 In the **Navigation** pane, expand **Locales** > ***Locale_name*** where you want to assign an organization.
Step 4 Click the **Assign Organization** link.
Step 5 In the **Assign Organization** dialog box, complete the following:
a) Expand **root** to view the organizations.
b) Check the appropriate check boxes.
Step 6 Click **OK**.

Deleting an Organization from a Locale

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **Access Control** subtab.
Step 3 In the **Navigation** pane, expand **Locales**.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 In the **Assigned Organizations** area, click the organization you want to delete.
Step 6 Click the **Delete Organization** link.
Step 7 In the **Confirm** dialog box, click **Yes**.

Configuring Locally Authenticated User Accounts

Creating a User Account

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.

Step 2 In the **Navigation** pane, click the **Access Control** subtab.

Step 3 In the **Navigation** pane, click the **Locally Authenticated Users** node.

Step 4 In the **Work** pane, click the **Create Locally Authenticated Users** link.

Step 5 In the **Properties** area, complete the following fields:

Name	Description
Login ID field	The log in name. This name must be unique and meet the following guidelines and restrictions for Cisco VNMC user accounts: • The login ID can be between 1 and 32 characters, including the following: ◦ Any alphabetic character ◦ Any digit ◦ _ (underscore) ◦ - (dash) ◦ @ • The user name for each user account cannot be all-numeric. • The user name cannot start with a number. After you save the user name, it cannot be changed. You must delete the user account and create a new one. You can create up to 48 user accounts for a single Cisco VNMC instance.
Description field	A description of the user.
First Name field	The first name of the user. This field can contain up to 32 characters.

Name	Description
Last Name field	The last name of the user. This field can contain up to 32 characters.
Email field	The email address of the user.
Phone field	The telephone number of the user.
Password field	The password associated with this account. For maximum security, each password must be strong. If the **Password Strength Check** checkbox is checked, the system rejects any password that does not meet the following requirements: • The password must contain a minimum of 8 characters • The password must contain at least three of the following: ◦ Lower case letters ◦ Upper case letters ◦ Digits ◦ Special characters • The password must not contain a character that is repeated more than 3 times consecutively, like aaabbb. • The password must not be the user name or the reverse of the user name. • The password must pass a password dictionary check. For example, the password must not be based on a standard dictionary word. • The password must not contain the following symbols: $ (dollar sign), ? (question mark), and = (equals sign). • The password should not be blank for local user and admin accounts. **Note** The password strength check box on the **Locally Authenticated Users** pane can be checked off, so that the password is not restricted to be strong. It must, however, contain a minimum of 8 characters. The password field is not a required field and a user can be created without providing a password.

Name	Description
Confirm Password field	The password is entered here a second time for confirmation purposes.
Password Expires check box	The password expiration date.

Step 6 In the **Roles/Locales** tab area, complete the following fields:

Name	Description
Assigned Role area	The area in which you manage roles. The **Assigned Roles** area contains the following check boxes: • **aaa** • **admin** • **network** • **operations** • **read-only** When a check box is checked, the user is assigned that role.
Assigned Locale area	The area in which you manage locales. The **Assigned Locales** area contains the assigned locales check boxes. When a check box is checked, the user is assigned to that locale.

Step 7 In the **SSH** tab area, complete the following fields:

Name	Description
Key	The SSH key. **Note** When you choose the **Key** radio button, the **SSH Data** field is displayed in the area.
Password	The SSH password.

Step 8 Click **OK**.

Changing the Locales Assigned to a Locally Authenticated User Account

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **Access Control** subtab.
Step 3 In the **Navigation** pane, expand the **Locally Authenticated Users** node.
Step 4 Click the *User_name* you want to modify.
Step 5 In the **Work** pane, click the **General** tab.
Step 6 In the **Work** pane, click the **Roles/Locales** tab.
Step 7 In the **Assigned Locale(s)** area, do the following:

- To assign a new locale to the user account, check the appropriate check boxes.
- To remove a locale from the user account, uncheck the appropriate check boxes.

Step 8 Click **Save**.

Changing the Roles Assigned to a Locally Authenticated User Account

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **Access Control** subtab.
Step 3 In the **Navigation** pane, expand the **Locally Authenticated Users** node.
Step 4 Click the *User_name* you want to modify.
Step 5 In the **Work** pane, click the **General** tab.
Step 6 Click the **Roles/Locales** tab.
Step 7 In the **Assigned Role(s)** area, do the following:

- To assign a new role to the user account, check the appropriate check boxes.
- To remove a role from the user account, uncheck the appropriate check boxes.

Step 8 Click **Save**.

Monitoring User Sessions

You can monitor a Cisco VNMC session for both locally authenticated users and remotely authenticated users.

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.

Step 2 In the **Navigation** pane, click the **Access Control** subtab.

Step 3 In the **Navigation** pane click and expand one of the following nodes:

- **Locally Authenticated Users**
- **Remotely Authenticated Users**

Step 4 Select a *User_name* to monitor.

Step 5 In the **Work** pane, click the **Sessions** tab to view the user session.

Name	Description
User column	The username that is involved in the session.
Host column	The IP address from which the user is logged in.
Login Time column	The date and time the session started.
UI column	The user interface used to create this user login session. This can be: • **web**—GUI login • **shell**—CLI login • **ep**—end point • **none**
Terminal Type column	The kind of terminal through which the user is logged in.

CHAPTER 5

Configuring Trusted Points

This chapter includes the following sections:

Trusted Points

When setting up LDAP over Secure Sockets Layer (SSL) protocol for Cisco VNMC user authentication, you need to create a trusted point for each LDAP server. The certificate in the trust point can be any one of the following:

- The certificate of the certificate authority (CA) that issued the LDAP server certificate.
- If the certificate authorities (CAs) are organized in a hierarchy, the certificate of any of the CAs in the hierarchy.
- The certificate of the LDAP server.

Configuring Trusted Points

Creating a Trusted Point

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.

Step 2 In the **Navigation** pane, click the **Access Control** subtab.

Step 3 In the **Navigation** pane, click the **Trusted Point** node.

Step 4 In the **Work** pane, click the **Create Trusted Point** link.

Step 5 In the **Create Trusted Point** dialog box, complete the following fields:

Name	Description
Name field	The name of the trusted point. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved. **Note** You cannot change this name after the object has been created.
Certificate Chain field	The certificate information for this trusted point. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon. You cannot change this description after it is saved.

Step 6 Click **OK**.

Editing a Trusted Point

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **Access Control** subtab.
Step 3 In the **Navigation** pane, click the **Trusted Point** node.
Step 4 In the **Work** pane, click the *Trusted Point_name* you want to edit.
Step 5 Click the **Edit** link.
Step 6 In the **Edit** dialog box, modify the certificate chain as appropriate.
Step 7 Click **OK**.

Deleting a Trusted Point

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **Access Control** subtab.
Step 3 In the **Navigation** pane, click the **Trusted Point** node.
Step 4 In the **Work** pane, click the trusted point you want to delete.
Step 5 Click the **Delete** link.
Step 6 In the **Confirm** dialog box, click **OK**.

CHAPTER 6

Configuring VNMC Profiles

This chapter includes the following sections:

VNMC Profiles

Cisco VNMC profiles are configurable.

In Cisco VNMC, there is a default profile that exists. Default profiles are system generated and can be modified, but they cannot be deleted. The administrator can add syslog policies, core policies, fault policies, log policies, and the time zone. DNS and NTP policies can be created also. Configured policies can be assigned to the VNMC profile.

In the VNMC profile, there is a pre-configured DNS domain name when the system is configured at boot configuration. That domain is displayed in the Cisco VNMC instance. New DNS domains cannot be created. However the domain name description can be modified.

Cisco VNMC does not support the creation of additional VNMC profiles.

Policies in VNMC Profiles

You can create multiple policies and assign them to the VNMC profile. Policies for the VNMC profile are created and deleted on the **VNMC Profile** tab. Policies can be assigned to the VNMC profile. VNMC profile uses name resolution to resolve policy assignments. For details, see Name Resolution in a Multi-tenancy Environment, on page 74.

The following policies created under root only, in the Device Policies area, will be visible in the VNMC profile:

- Core file policy
- Fault policy
- Logging policy

- Syslog policy

Policies created under root are visible to both the VNMC profile and the Device profile.

DNS server, NTP server and domain names can be assigned as inline policies. A time zone setting can also be assigned to the profile.

When the system boots up, the following policies already have existing default policies:

- Fault policy
- Logging policy
- Syslog policy

The default policies cannot be deleted but may be modified.

Configuring Policies

Configuring a Core File Policy

Adding a Core File Policy to the VNMC Profile

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.

Step 2 In the **Navigation** pane, click the **VNMC Profile** subtab.

Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **VNMC Policies**.

Step 4 In the **Navigation** pane, click **Core File**.

Step 5 In the **Work** pane, click the **Add Core File Policy** link.

Step 6 In the **Add Core File Policy** dialog box, complete the following fields:

Name	Description
Name field	The name of the core file policy. This name can be between 1 and 511 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been created.
Description field	The description of the core file policy. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon. You cannot change this description after it is saved.

Name	Description
Admin State drop-down list	The state of the core file policy. It can be one of the following states: • **Enabled**—Enables the core file policy. TFTP is used. • **Disabled**—Disables the core file policy.
Hostname field	The hostname or IP address to connect using TFTP. **Note** If you use a hostname rather than an IP address, you must configure a DNS server in Cisco VNMC.
Port field	The port number to send the core dump file to.
Protocol field	The protocol used to export the core dump file. This field cannot be edited.
Path field	The path to use when storing the core dump file on a remote system. The default path is /tftpboot. An example path would be /tftpboot/test, where test is the sub-folder.

Step 7 Click **OK**.

Editing a Core File Policy for VNMC Profile

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **VNMC Profile** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **VNMC Policies**.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 On the **General** tab, click the core file policy you want to edit.
Step 6 Click the **Edit** link.
Step 7 In the **Edit** dialog box, modify the following fields as appropriate:

Name	Description
Name field	The name of the core file policy.
Description field	A description of the core file policy.

Name	Description
Admin State drop-down list	A list of administrative states. This can be one of the following states: • **enabled**—Enables the core file policy. • **disabled**—Disables the core file policy.
Hostname field	The hostname or IP address. **Note** If you use a hostname rather than an IP address, you must configure a DNS server.
Port field	The port number used when exporting the core dump file. The default path is /tftpboot. To mention a sub folder under tftpboot, use, for example, /tftpboot/test.
Protocol field	The protocol used to export the core dump file.
Path check box	The path to use when storing the core dump file on the remote system.

Step 8 Click **OK**.

Deleting a Core File Policy from the VNMC Profile

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **VNMC Profile** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **VNMC Policies**.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 On the **General** tab, click the core file policy you want to delete.
Step 6 Click the **Delete** link.
Step 7 In the **Confirm** dialog box, click **Yes**.

Configuring a Fault Policy

Adding a Fault Policy to the VNMC Profile

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.

Step 2 In the **Navigation** pane, click the **VNMC Profile** subtab.

Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **VNMC Policies**.

Step 4 In the **Navigation** pane, click **Fault**.

Step 5 In the **Work** pane, click the **Add Fault Policy** link.

Step 6 In the **Add Fault Policy** dialog box, complete the following fields:

Name	Description
Name field	A user-defined name for the fault policy. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.
Description field	A user-defined description of the fault policy.
Flapping Interval spinbox	Flapping occurs when a fault is raised and cleared several times in rapid succession. To prevent this, the system does not allow a fault to change its state until this amount of time has elapsed since the last state change. If the condition reoccurs during the flapping interval, the fault returns to the active state. If the condition does not reoccur during the flapping interval, the fault is cleared. What happens at that point depends on the setting in the **Clear Faults Retention Action** field. The number of hours, minutes, and seconds that should pass before the system allows a fault to change its state. The default flapping interval is 10 seconds.
Clear Faults Retention Action drop-down list	The state of the clear faults retention action. It can be one of the following states: • **retain**—Retains the cleared faults section. • **delete**—The system immediately deletes all fault messages as soon as they are marked as cleared.

Name	Description
Clear Faults Retention Interval radio-button	The state of the clear faults retention interval. It can be one of the following states: • **Forever**—The system leaves all cleared fault messages regardless of how long they have been in the system. • **Other**—The system displays the **dd:hh:mm:ss** spinbox for selection of the number of days, hours, minutes, and seconds that should pass before the system deletes a cleared fault message. The default retention interval is 1 hour.

Step 7 Click **OK**.

Editing a Fault Policy for a VNMC Profile

Note When the system boots up, a default policy already exists. The default policy cannot be deleted but may be modified.

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **VNMC Profile** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **VNMC Policies**.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 On the **General** tab, click the fault policy you want to edit.
Step 6 In the **Work** pane, click the **Edit** link.
Step 7 In the **Edit** dialog box, modify the appropriate fields:

Name	Description
Name field	The name of the fault policy.
Description field	A description of the fault policy.

Name	Description
Flapping Interval spinbox	The spinbox that lists flapping intervals. Use the box to set the interval. Flapping occurs when a fault is raised and cleared several times in rapid succession. To prevent this, the system does not allow a fault to change its state until this amount of time has elapsed since the last state change. The interval is the number of hours, minutes, and seconds that should pass before the system allows a fault to change its state. If the condition reoccurs during the flapping interval, the fault returns to the active state. If the condition does not reoccur during the flapping interval, the fault is cleared. What happens at that point depends on the setting in the **Clear Faults Retention Action** field. The default flapping interval is 10 seconds.
Clear Faults Retention Action drop-down list	The list that contains fault retention actions. Use the list to set an action. This can be one of the following actions: • **retain**—The system retains fault messages. • **delete**—The system immediately deletes all fault messages as soon as they are marked as cleared.
Clear Faults Retention Interval radio-button	The control that sets the retention interval. Use the control to set the interval. This can be one of the following values: • **forever**—The system leaves all cleared fault messages regardless of how long they have been in the system. • **other**—The system displays the **dd:hh:mm:ss** spinbox for selection of the number of days, hours, minutes, and seconds that should pass before the system deletes a cleared fault message. The default retention interval is 1 hour.

Step 8 Click **OK**.

Deleting a Fault Policy from the VNMC Profile

Note When the system boots up, a default policy already exists. The default policy cannot be deleted but may be modified.

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **VNMC Profile** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **VNMC Policies**.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 On the **General** tab, click the fault policy you want to delete.
Step 6 Click the **Delete** link.
Step 7 In the **Confirm** dialog box, click **OK**.

Configuring a Logging Policy

Adding a Logging Policy to the VNMC Profile

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **VNMC Profile** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **VNMC Policies**.
Step 4 In the **Navigation** pane, click **Log File**.
Step 5 In the **Work** pane, click the **Add Logging Policy** link.
Step 6 In the **Add Logging Policy** dialog box, complete the following fields:

Name	Description
Name field	The name of the logging policy. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.
Description field	A description of the logging policy.

Name	Description
Log Level drop-down list	A list of logging severity levels. This can be one of the following levels: • **debug0** • **debug1** • **debug2** • **debug3** • **debug4** • **info** • **warn** • **minor** • **major** • **crit** The default log level is **info**.
Backup Files Count field	The number of backup files that are filled before they are overwritten. The range is 1 to 9 files. The default is 2 files.
File Size (bytes) field	The backup file size. The range is 1MB to 100MB. The default file size is 5MB.

Step 7 Click **OK**.

Editing a Logging Policy for VNMC Profile

Note When the system boots up, a default policy already exists. The default policy cannot be deleted but may be modified.

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.

Step 2 In the **Navigation** pane, click the **VNMC Profile** subtab.

Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **VNMC Policies**.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 On the **General** tab, click the logging policy you want to edit.

Step 6 Click the **Edit** link.

Step 7 In the **Edit** dialog box, modify any of the following fields:

Name	Description
Name field	The name of the logging policy. This field cannot be edited.
Description field	A description of the logging policy.
Log Level drop-down list	A list of logging levels. This can be one of the following levels: • **debug0** • **debug1** • **debug2** • **debug3** • **debug4** • **info** • **warn** • **minor** • **major** • **crit** The default log level is **info**.
Backup Files Count field	The number of backup files that are filled before they are overwritten. The range is 1 to 9 files. The default is 2 files.
File Size (bytes) field	The backup file size. The range is 1MB to 100MB. The default file size is 5MB.

Step 8 Click **OK**.

Deleting a Logging Policy from the VNMC Profile

Note When the system boots up, a default policy already exists. The default policy cannot be deleted but may be modified.

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **VNMC Profile** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **VNMC Policies**.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 On the **General** tab, click the logging policy you want to delete.
Step 6 Click the **Delete** link.
Step 7 In the **Confirm** dialog box, click **Yes**.

Configuring Syslog Policy

Adding a Syslog Policy to the VNMC Profile

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **VNMC Profile** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **VNMC Policies**.
Step 4 In the **Navigation** pane, click **Syslog** to view the **Syslog** work pane.
Step 5 In the **Work** pane, click the **Add Syslog** link.
Step 6 In the **Add Syslog** dialog box, complete the following fields:
a) In the **General** tab area, complete as appropriate:

Table 4: General Tab

Name	Description
Name field	The name of the syslog policy. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.
Description field	The description of the syslog policy.
Port field	The TCP or UDP port where syslog messages are sent. You cannot edit this field.

b) In the **Local Destinations** tab area, complete as appropriate in the **Console** area, **Monitor** area, and **File** area:

Table 5: Console Area

Name	Description
Admin State radio button	The administrative state of the policy. It can be one of the following states: • **enabled** • **disabled**
Level radio button	The message level. It can be one of the following levels: • **alerts** • **critical** • **emergencies** If the **Admin State** is enabled, select the lowest message level that you want displayed. The system displays that level and above on the console.

Table 6: Monitor Area

Name	Description
Admin State radio button	The administrative state of the policy. It can be one of the following states: • **enabled** • **disabled**
Level drop-down list	The message levels. It can be one of the following levels: • **emergencies (0)** • **alerts (1)** • **critical (2)** • **errors (3)** • **warnings (4)** • **notifications (5)** • **information (6)** • **debugging (7)** If the **Admin State** is enabled, select the lowest message level that you want displayed. The system displays that level and above on the console.

Table 7: File Area

Name	Description
Admin State radio button	The administrative state of the policy. It can be one of the following states: • **enabled** • **disabled**

Name	Description
Level drop-down list	The message levels. It can be one of the following levels: • **emergencies (0)** • **alerts (1)** • **critical (2)** • **errors (3)** • **warnings (4)** • **notifications (5)** • **information (6)** • **debugging (7)** If the **Admin State** is enabled, select the lowest message level that you want displayed. The system displays that level and above on the console.
File Name field	The name of the file in which messages are logged.
Size (Bytes) field	The maximum size, in bytes, the file can be before the system begins to over-write messages.

Step 7 Click **OK**.

Editing a Syslog Policy for VNMC Profile

Note When the system boots up, a default policy already exists. The default policy cannot be deleted but may be modified.

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.

Step 2 In the **Navigation** pane, click the **VNMC Profile** subtab.

Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **VNMC Policies** > **Syslog**.

Step 4 Click the **Syslog Policies** node.

Step 5 In the **Work** pane, click the syslog policy you want to edit.

Step 6 Click the **Edit** link.

Step 7 In the **Edit** dialog box, do the following:

a) In the **General** tab area, edit the appropriate fields:

Name	Description
Name field	The name of the syslog policy.
Description field	The description of the syslog policy.
Admin State drop-down list	The administrative state of the policy. It can be one of the following states: • **enabled** • **disabled**
Port field	The TCP or UDP port where syslog messages are sent.

b) In the **Local Destinations** tab area, edit the appropriate fields in the **Console** area:

Name	Description
Admin State radio button	The administrative state of the policy. It can be one of the following states: • **enabled** • **disabled**
Level radio button	The message level. It can be one of the following levels: • **alerts** • **critical** • **emergencies** If the **Admin State** is enabled, select the lowest message level that you want displayed. The system displays that level and above on the console.

c) In the **Local Destinations** tab area, edit the appropriate fields in the **Monitor** area:

Name	Description
Admin State radio button	The administrative state of the policy. It can be one of the following states: • **enabled** • **disabled**
Level drop-down list	The message levels. It can be one of the following levels: • **emergencies (0)** • **alerts (1)** • **critical (2)** • **errors (3)** • **warnings (4)** • **notifications (5)** • **information (6)** • **debugging (7)** If the **Admin State** is enabled, select the lowest message level that you want displayed. The system displays that level and above on the console.

d) In the **Local Destinations** tab area, edit the appropriate fields in the **File** area:

Name	Description
Admin State radio button	The administrative state of the policy. It can be one of the following states: • **enabled** • **disabled**

Name	Description
Level drop-down list	The message levels. It can be one of the following levels: • **emergencies (0)** • **alerts (1)** • **critical (2)** • **errors (3)** • **warnings (4)** • **notifications (5)** • **information (6)** • **debugging (7)** If the **Admin State** is enabled, select the lowest message level that you want displayed. The system displays that level and above on the console.
File Name field	The name of the file in which messages are logged.
Size (Bytes) field	The maximum size, in bytes, the file can be before the system begins to over-write messages.

Step 8 Click **OK**.

Deleting a Syslog Policy from a VNMC Profile

Note When the system boots up, a default policy already exists. The default policy cannot be deleted but may be modified.

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **VNMC Profile** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **VNMC Policies** > **Syslog**.
Step 4 In the **Work** pane, click the syslog policy you want to delete.
Step 5 Click the **Delete** link.
Step 6 In the **Confirm** dialog box, click **Yes**.

Adding a Syslog Server to the VNMC Profile

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **VNMC Profile** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **VNMC Policies**.
Step 4 Click the **Syslog** node.
Step 5 In the **Work** pane, click the **Add Syslog** link.
Step 6 In the **Add Syslog** dialog box, click the **Servers** tab.
Step 7 Click the **Add Syslog Servers** link.
Step 8 In the **Add Syslog Server** dialog box, complete the following fields:

Name	Description
Server Type field	The type of server. It can be one of the following types: • **primary** • **secondary** • **tertiary**
Hostname/IP address field	The hostname or IP address where the syslog file resides.

Name	Description
Severity field	The severity level. It can be one of the following levels: • **emergencies (0)** • **alerts (1)** • **critical (2)** • **errors (3)** • **warnings (4)** • **notifications (5)** • **information (6)** • **debugging (7)**
Forwarding Facility field	The forwarding facility. It can be one of the following types: • **auth** • **authpriv** • **cron** • **daemon** • **ftp** • **kernel** • **local0** • **local1** • **local2** • **local3** • **local4** • **local5** • **local6** • **lpr** • **mail** • **news** • **syslog** • **user** • **uucp**

Name	Description
Admin State field	The administrative state of the policy. It can be one of the following states: • **enabled** • **disabled**

Step 9 Click **OK**.

Editing a Syslog Server for VNMC Profile

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.

Step 2 In the **Navigation** pane, click the **VNMC Profile** subtab.

Step 3 In the **Navigation** pane, expand **root** > **Policies** > **Syslog Policies** > ***Syslog Policy_name*** where you want to edit a syslog server.

Step 4 In the **Work** pane, click the server you want to edit.

Step 5 Click the **Edit** link.

Step 6 In the **Edit Syslog Server** dialog box, edit the appropriate fields:

Name	Description
Server Type column	The type of server. It can be one of the following types: • **primary** • **secondary** • **tertiary**
Hostname column	The hostname or IP address where the syslog file resides.
Admin State column	The administrative state of the policy. It can be one of the following states: • **enabled** • **disabled**

Name	Description
Severity column	The severity level. It can be one of the following levels: • **emergencies (0)** • **alerts (1)** • **critical (2)** • **errors (3)** • **warnings (4)** • **notifications (5)** • **information (6)** • **debugging (7)**
Forwarding Facility column	The forwarding facility. It can be one of the following types: • **auth** • **authpriv** • **cron** • **daemon** • **ftp** • **kernel** • **local0** • **local1** • **local2** • **local3** • **local4** • **local5** • **local6** • **lpr** • **mail** • **news** • **syslog** • **user** • **uucp**

Step 7 Click **OK**.

Deleting a Syslog Server from a VNMC Profile

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **VNMC Profile** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **VNMC Policies**.
Step 4 In the **Navigation** pane, click the **Syslog** node.
Step 5 In the **Work** pane, click the **General** tab.
Step 6 On the **General** tab, click the **Add Syslog** link.
Step 7 In the **Add Syslog** dialog box, click the **Servers** tab.
Step 8 On the **Servers** tab, click the syslog server you want to delete.
Step 9 Click the **Delete** link.
Step 10 In the **Confirm** dialog box, click **Yes**.

Configuring the Default Profile

Editing the VNMC default Profile

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **VNMC Profile** subtab.
Step 3 In the **Navigation** pane, expand **root** > **VNMC Profile**.
Step 4 Click the **default** profile node .
Step 5 In the **Work** pane, **General** tab area, change the following fields as appropriate:

Name	Description
Name field	A system-defined name for this default profile.
Description field	A user-defined description of the profile.
Time Zone drop-down list	A list of time zones for user selection.

Step 6 In the **Work** pane **Policy** tab area, do the following:

a) In the **DNS Servers** area, change the following fields as appropriate:

Name	Description
Add DNS Server link	Opens a dialog box that allows you to specify a new DNS server.
Delete link	Deletes the DNS server IP address selected in the **IP Address** table.
Up and **Down** arrows	Changes the priority of the selected DNS Server IP address.
IP Address table	Contains the IP addresses for the DNS servers configured in the system. VNMC uses the DNS servers in the order they appear in the table.

b) In the **NTP Servers** area, change the following fields as appropriate:

Name	Description
Add NTP Server link	Opens a dialog box that allows you to specify a new NTP server.
Delete link	Deletes the NTP server hostname selected in the **Hostname** table.
Up and **Down** arrows	Changes the priority of the selected NTP Server hostname.
Hostname table	Contains the NTP server hostnames configured in the system. VNMC uses the NTP server hostnames in the order they appear in the table.

c) In the **DNS Domains** area, change the following fields as appropriate:

Name	Description
Edit link	Edits the DNS domain name selected in the **DNS Domains** table. The **default** DNS name cannot be edited.
DNS Domains table	Contains the default DNS domain name and domain in the system.

d) In the Log area, change the following fields as appropriate:

Name	Description
Syslog area	The syslog policies associated with this profile can be selected, added, or edited. Contains the **Resolved Policy** field.
Fault area	The fault policies associated with this profile can be selected, added, or edited. Contains the **Resolved Policy** field.
Core File area	The core file policies associated with this profile can be selected, added, or edited. Contains the **Resolved Policy** field.
Log File area	The log file policies associated with this profile can be selected, added, or edited. Contains the **Resolved Policy** field.

Step 7 Click **OK**.

Configuring a DNS Server

Adding a DNS Server

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **VNMC Profile** subtab.
Step 3 In the **Navigation** pane, expand **root** > **VNMC Profile**.
Step 4 In the **Navigation** pane, click **default**.
Step 5 In the **Work** pane, click the **Policy** tab.
Step 6 In the **DNS Servers** area, click the **Add DNS Server** link.
Step 7 In the **Add DNS Server** dialog box, complete the following field:

Name	Description
DNS IP Address field	The DNS server IP address.

Step 8 In the **Add DNS Server** dialog box, click **OK**.

Note Up to four DNS IP addresses are accepted.

Deleting a DNS Server

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **VNMC Profile** subtab.
Step 3 In the **Navigation** pane, expand **root** > **VNMC Profile**.
Step 4 In the **Navigation** pane, click *default*.
Step 5 In the **Work** pane, click the **Policy** tab.
Step 6 In the **DNS Servers** area, click the IP address you want to delete.
Step 7 Click the **Delete** link.
Step 8 In the **Confirm** dialog box, click **Yes**.
Step 9 In the **Work** pane, click **Save**.

Configuring an NTP Server

Adding an NTP Server

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **VNMC Profile** subtab.
Step 3 In the **Navigation** pane, expand **root** > **VNMC Profile**.
Step 4 In the **Navigation** pane, click the **default** profile.
Step 5 In the **Work** pane, click the **Policy** tab.
Step 6 In the **NTP Servers** area, click the **Add NTP Server** link.
Step 7 In the **Add NTP Server** dialog box, complete the following field:

Name	Description
Host Name field	The name of the NTP server.

Note Up to four NTP server hostnames are accepted. The name on top is the primary hostname. You can use the **Up** and **Down** arrows to rearrange the names.

Step 8 Click **OK**.

Deleting an NTP Server

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **VNMC Profile** subtab.
Step 3 In the **Navigation** pane, expand **root** > **VNMC Profile**.
Step 4 In the **Navigation** pane, click *default*.
Step 5 In the **Work** pane, click the **Policy** tab.
Step 6 In the **NTP Servers** area, click the server that you want to delete.
Step 7 In the **NTP Servers** area, click the **Delete** link.
Step 8 In the **Confirm** dialog box, click **Yes**.

Configuring a DNS Domain

Editing a DNS Domain

Caution Changing the DNS domain will cause connectivity loss.

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **VNMC Profile** subtab.
Step 3 In the **Navigation** pane, expand **root** > **VNMC Profile** > ***default***.
Step 4 In the **Work** pane, click the **Policy** tab.
Step 5 In the **DNS Domains** area, select the *DNS_Domains_name* you want to edit.
Step 6 Click the **Edit** link.
Step 7 In the **Edit DNS Domains** dialog box, edit the description field as appropriate:

Name	Description
Name field	The name of the policy. **Note** You cannot edit the **Name** field for the default domain.

Name	Description
Domain Name field	The domain name.

Step 8 In the **Edit DNS Domains** dialog box, click **OK**.

Step 9 In the **Policy** tabs area, click **Save**.

CHAPTER 7

Configuring VM Managers

This chapter includes the following sections:

VNMC VM Manager vCenter Connection

VNMC VM Manager connects to vCenter on port 80. A vCenter extension file is required to establish a connection between VM Manager and vCenter. The extension file is exported from Cisco VNMC and linked on the VM Managers tab. You install it as a plugin on all the vCenter servers to which you want to connect.

Configuring VM Managers from the Administration Tab

Adding a VM Manager

Before You Begin

A vCenter extension file is required to establish a secure connection between the vCenter and the VM Manager. Export the vCenter extension file by clicking the **Export vCenter Extension** link, and installing it as a plugin on all the vCenter servers.

Note On the **Plug-In Manager** page of the vCenter, scroll to the end of the page, and right-click to view the **New Plug-in** menu.

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.

Step 2 In the **Navigation** pane, click the **VM Managers** subtab.

Step 3 In the **Navigation** pane, click the **VM Managers** node to view the **VM Managers** work pane.

Step 4 In the **Work** pane, click the **Add VM Manager** link.

Step 5 In the **Add VM Manager** dialog box, complete the following fields:

Name	Description
Name field	The name of the VM Manager. This name can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon. You cannot change this description after it is saved.
Description field	A description of the VM Manager. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon. You cannot change this description after it is saved.
Hostname/IP Address field	The host name or IP address of the VM Manager.

Step 6 Click **OK**.

Note Once a VM Manager is added, Cisco VNMC fetches the hypervisor/VMs and displays it in the **Resource Manager** > **Resources** tab. Only VMs with Cisco Nexus 1000V Series switch port profiles attached are fetched.

Editing a VM Manager

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.

Step 2 In the **Navigation** pane, click the **VM Managers** subtab.

Step 3 In the right **Work** pane, click the VM Manager you want to edit.

Step 4 Click the **Edit** link.

Step 5 In the **Edit VM Manager** dialog box, edit the appropriate information as required.

Name	Description
Name field	The name of the VM Manager. This field cannot be edited.
Description field	A description of the VM Manager.
Hostname/IP Address field	The hostname or IP address of the VM Manager. This field cannot be edited.
Admin State field	The administrative state for the VM Manager. This can be one of the following states: • **enable** • **disable** When a vCenter is added to Cisco VNMC, with the **enable** option, the system fetches all the VM inventory from vCenter. Any changes occurring to the VMs on vCenter are also fetched. When a vCenter is added to Cisco VNMC, with the **disable** option, the system displays all the discovered VMs from vCenter. Any changes occurring to the VMs on the vCenter are not fetched. The changes will be fetched by Cisco VNMC when the admin state is changed to **enable**.
Type field	The vendor for this VM Manager.
Version field	The version of the VM Manager.
Operational State field	This can be: • **up** • **unreachable** • **bad-credentials** • **comm-error** • **admin-down** • **unknown**
Operational State Reason field	The operational state.

Step 6 Click **OK**.

Deleting a VM Manager

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **VM Managers** subtab.
Step 3 In the **Work** pane, click the **VM Managers** tab.
Step 4 In the **VM Managers** table, click the VM Manager you want to delete.
Step 5 Click the **Delete** link.
Step 6 In the **Confirm** dialog box, click **Yes**.

Configuring VM Managers from the Resource Management Tab

Adding a VM Manager

Before You Begin

A vCenter extension file is required to establish a secure connection between the vCenter and the VM Manager. Export the vCenter extension file by clicking the **Export vCenter Extension** link, and installing it as a plugin on all the vCenter servers.

Note On the **Plug-In Manager** page of the vCenter, scroll to the end of the page, and right-click to view the **New Plug-in** menu.

Procedure

Step 1 In the **Navigation** pane, click the **Resource Management** tab.
Step 2 In the **Navigation** pane, click the **Resources** subtab.
Step 3 In the **Navigation** pane, click **Virtual Machines**.
Step 4 In the **Navigation** pane, click the **VM Managers** node.
Step 5 In the **Work** pane, click the **Add VM Manager** link.
Step 6 In the **Add VM Manager** dialog box, complete the following fields:

Name	Description
Name field	The name of the VM Manager. This name can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon. You cannot change this description after it is saved.
Description field	A description of the VM Manager. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon. You cannot change this description after it is saved.
Hostname/IP Address field	The host name or IP address of the VM Manager.

Step 7 Click **OK**.

Note Once a VM Manager is added, Cisco VNMC fetches the hypervisor/VMs and displays it in the **Resource Manager** > **Resources** tab. Only VMs with Cisco Nexus 1000V Series switch port profiles attached are fetched.

Editing a VM Manager

Procedure

Step 1 In the **Navigation** pane, click the **Resource Management** tab.

Step 2 In the **Navigation** pane, click the **Resources** subtab.

Step 3 In the **Navigation** pane, click **Virtual Machines**.

Step 4 In the **Navigation** pane, click the **VM Managers** node.

Step 5 In the right **Work** pane, click the VM Manager you want to edit.

Step 6 Click the **Edit** link.

Step 7 In the **Edit VM Manager** dialog box, edit the appropriate information as required.

Name	Description
Name field	The name of the VM Manager. This field cannot be edited.
Description field	A description of the VM Manager.
Hostname/IP Address field	The hostname or IP address of the VM Manager. This field cannot be edited.

Name	Description
Admin State field	The administrative state for the VM Manager. This can be one of the following states: • **enable** • **disable** When a vCenter is added to Cisco VNMC, with the **enable** option, the system fetches all the VM inventory from vCenter. Any changes occurring to the VMs on vCenter are also fetched. When a vCenter is added to Cisco VNMC, with the **disable** option, the system displays all the discovered VMs from vCenter. Any changes occurring to the VMs on the vCenter are not fetched. The changes will be fetched by Cisco VNMC when the admin state is changed to **enable**.
Type field	The vendor for this VM Manager.
Version field	The version of the VM Manager.
Operational State field	This can be: • **up** • **unreachable** • **bad-credentials** • **comm-error** • **admin-down** • **unknown**
Operational State Reason field	The operational state.

Step 8 Click **OK**.

Deleting a VM Manager

Procedure

Step 1 In the **Navigation** pane, click the **Resource Management** tab.
Step 2 In the **Navigation** pane, click the **Resources** subtab.
Step 3 In the **Navigation** pane, click **Virtual Machines**.
Step 4 In the **Work** pane, click the **VM Managers** tab.
Step 5 In the **VM Managers** table, click the VM Manager you want to delete.
Step 6 Click the **Delete** link.
Step 7 In the **Confirm** dialog box, click **Yes**.

CHAPTER 8

Configuring Tenants

This chapter includes the following sections:

Tenant Management

Tenant Management and Multi-tenancy

Cisco VNMC provides the ability to achieve multi-tenancy. Multi-tenancy enables the division of large physical infrastructures into logical entities called organizations. As a result, you can achieve logical isolation between organizations without providing a dedicated physical infrastructure for each organization.

The administrator can assign unique resources to each tenant through the related organization in the multi-tenant environment. These resources can include different policies, pools, device profiles, firewalls and such. The administrator can use locales to assign or restrict user privileges and roles by organization if access to certain organizations need to be restricted.

Cisco VNMC provides a strict organizational hierarchy as follows:

1. Root
2. Tenant
3. Data Center
4. Application
5. Tier

The root can have multiple tenants. Each tenant can have multiple data centers. Each data center can have multiple applications, and each application can have multiple tiers.

The policies and pools created at the root level are systemwide and are available to all organizations in the system. However, any policies and pools created in an organization are only available to organizations that are below it in the same hierarchy.

For example, if a system has tenants named Company A and Company B, Company A cannot use any policies created in the Company B organization. Company B cannot access any policies created in the Company A organization. However, both Company A and Company B can use policies and pools in the root organization.

Name Resolution in a Multi-tenancy Environment

In a multi-tenant environment, Cisco VNMC uses the hierarchy of an organization to resolve the names of policies and resource pools. The steps Cisco VNMC takes to resolve the names of policies and resource pools are as follows:

1. Cisco VNMC checks the policies and pools for the specified name within an organization assigned to the device profile or security policy.
2. If the policy or pool is found, Cisco VNMC uses that policy.
3. If the policy or pool does not contain available resources at the local level, Cisco VNMC moves up the hierarchy to the parent organization and checks for a policy with the specified name. Cisco VNMC repeats this step until the search reaches the root organization.

Attention The object name reference resolution takes an object name and resolves an object from an organization container to the object with the same name which is closest in the tree up to the root of the tree. If an object with the specified name is not found, it uses a corresponding default object. For example, there is an SNMP policy under data center called MySNMP, and there is an SNMP policy in the tenant in the same tree that is also MySNMP. In this case, the user cannot explicitly select the MySNMP policy under tenant. If the user wants to select the SNMP policy under tenant, they must provide a unique name for the object in the given tree.

4. If the search reaches the root organization and an assigned policy or pool is not found, Cisco VNMC looks for a default policy or pool starting at the current level and going up the chain to the root level. If a default policy is found, Cisco VNMC uses it. If a policy is not available, a fault is generated.

Configuring Tenants

Creating a Tenant

Procedure

Step 1 In the **Navigation** pane, click the **Tenant Management** tab.
Step 2 In the **Navigation** pane, click the **root** node.
Step 3 In the **Work** pane, click the **Create Tenant** link.
Step 4 In the **Create Tenant** dialog box, complete the following fields:

Name	Description
Name field	The name of the Tenant. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.
Description field	A description of the Tenant. This name can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.

Step 5 Click **OK**.

Editing a Tenant

Procedure

Step 1 In the **Navigation** pane, click the **Tenant Management** tab.
Step 2 In the **Navigation** pane, click the **root** node.
Step 3 Click the *Tenant_name* you want to edit.
Step 4 In the **Work** pane, click the **Sub-Elements** tab.
Step 5 In the **Work** pane, click the **Edit Tenant** link.
Step 6 In the **Edit** dialog box, modify description.
Step 7 Click **OK**.

Deleting a Tenant

Attention When you delete an organization, all data contained under the organization is deleted, including sub-organizations, compute firewalls, resource pools, and policies.

Procedure

Step 1 In the **Navigation** pane, click the **Tenant Management** tab.
Step 2 In the **Navigation** pane, click the **root** node.
Step 3 In the **Work** pane, click the **Sub-Elements** tab.
Step 4 Click the tenant you want to delete.
Step 5 Click the **Delete** link.
Step 6 In the **Confirm** dialog box, click **Yes**.

Configuring Data Centers

Creating a Virtual Data Center

Procedure

Step 1 In the **Navigation** pane, click the **Tenant Management** tab.
Step 2 In the **Navigation** pane, expand **root** > ***Tenant_name*** where you want to create a virtual data center.
Step 3 In the **Work** pane, click the **Create Virtual Data Center** link.
Step 4 In the **Create Virtual Data Center** dialog box, complete the following fields:

Name	Description
Name field	The name of the Virtual Data Center. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.
Description field	A description of the Virtual Data Center. This name can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.

Step 5 Click **OK**.

Editing a Virtual Data Center

Procedure

Step 1 In the **Navigation** pane, click the **Tenant Management** tab.
Step 2 In the **Navigation** pane, expand **root** > ***tenant_name***.
Step 3 In the **Work** pane, click the **Sub-Elements** tab.
Step 4 On the **Sub-Elements** tab, click the virtual data center you want to edit.
Step 5 Click the **Edit** link.
Step 6 In the **Edit** dialog box, modify the description.
Step 7 Click **OK**.

Deleting a Virtual Data Center

Attention When you delete an organization, all data contained under the organization is deleted, including sub-organizations, compute firewalls, resource pools, and policies.

Procedure

Step 1 In the **Navigation** pane, click the **Tenant Management** tab.
Step 2 In the **Navigation** pane, expand **root** > ***Tenant_name*** where you want to delete a virtual data center.
Step 3 In the **Work** pane, click the **Sub-Elements** tab.
Step 4 In the **Work** pane, click the virtual data center you want to delete.
Step 5 Click the **Delete Virtual Data Center** link.
Step 6 In the **Confirm** dialog box, click **Yes**.

Configuring Applications

Creating an Application

Procedure

Step 1 In the **Navigation** pane, click the **Tenant Management** tab.

Step 2 In the **Navigation** pane, expand **root** > ***Tenant_name*** > ***Virtual Data Center_name*** where you want to create an application.

Step 3 In the **Work** pane, click the **Create Application** link.

Step 4 In the **Create Application** dialog box, complete the following fields:

Name	Description
Name field	The name of the Application. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.
Description field	A description of the Application. This name can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.

Step 5 Click **OK**.

Editing an Application

Procedure

Step 1 In the **Navigation** pane, click the **Tenant Management** tab.

Step 2 In the **Navigation** pane, click the **root** > ***Tenant_name*** > ***Virtual Data Center_name*** where you want to edit an application.

Step 3 In the **Work** pane, click the **Sub-Elements** tab.

Step 4 Click the *Application_name* you want to edit.

Step 5 Click the **Edit** link.

Step 6 In the **Edit** dialog box, modify the description.

Step 7 Click **OK**.

Deleting an Application

Attention When you delete an organization, all data contained under the organization is deleted, including sub-organizations, compute firewalls, resource pools, and policies.

Procedure

Step 1 In the **Navigation** pane, click the **Tenant Management** tab.

Step 2 In the **Navigation** pane, expand **root** > ***Tenant_name*** > ***Virtual Data Center_name*** where you want to delete an application.

Step 3 In the **Work** pane, click the **Sub-Elements** tab.

Step 4 In the **Work** pane, click the application you want to delete.

Step 5 Click the **Delete Application** link.

Step 6 In the **Confirm** dialog box, click **Yes**.

Configuring Tiers

Creating a Tier

Procedure

Step 1 In the **Navigation** pane, click the **Tenant Management** tab.

Step 2 In the **Navigation** pane, expand **root** > ***Tenant_name*** > ***Virtual Data Center_name*** > ***Application_name*** where you want to create a tier.

Step 3 In the **Work** pane, click the **Create Tier** link.

Step 4 In the **Create Tier** dialog box, complete the following fields:

Name	Description
Name field	The name of the Tier. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.
Description field	A description of the Tier. This name can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.

Step 5 Click **OK**.

Editing a Tier

Procedure

Step 1 In the **Navigation** pane, click the **Tenant Management** tab.

Step 2 In the **Navigation** pane, click the **root** node to expand.

Step 3 In the **Navigation** pane, click the *Tier_name* you want to edit.

Step 4 In the **Work** pane, click the **Properties** tab.

Step 5 In the **Description** field, modify the description.

Step 6 Click **OK**.

Deleting a Tier

Attention When you delete an organization, all data contained under the organization is deleted, including sub-organizations, compute firewalls, resource pools, and policies.

Procedure

Step 1 In the **Navigation** pane, click the **Tenant Management** tab.

Step 2 In the **Navigation** pane, expand **root** > *Tenant_name* > *Virtual Data Center_name* > *Application_name* where you want to delete a tier.

Step 3 In the **Work** pane, click the **Sub-Elements** tab.

Step 4 On the **Sub-Elements** tab, click the tier you want to delete.

Step 5 Click the **Delete Tier** link.

Step 6 In the **Confirm** dialog box, click **Yes**.

CHAPTER 9

Configuring Security Policies

This chapter includes the following sections:

Security Policies

Cisco VNMC security policies provide options to create security profiles and policies. A security profile and policies can be configured at any organizational level.

Security Profile

A Cisco VNMC security profile is a set of custom security attributes and one assigned policy set. The security profile is added to the port profile for the Nexus 1000V VSM. The port profile is assigned to the Nexus 1000V VSM vNic, making the security profile part of the virtual machine (VM). Adding a security profile to the VM allows the addition of custom attributes to the VM. Firewall rules can be written using custom attributes such that traffic between VMs can be allowed to pass or be dropped. You can also add security policies in the same GUI pane where you are adding security profiles.

There is a pre-configured default security profile at root level. The default security profile points to the default policy set. The default security profile can be edited but cannot be deleted.

Policies

A Cisco VNMC supports a number of policies. The policies are as follows:

1 Policy set—The policy set contains the policy, the rule, the zone, and the object group. Once the policy set is created, it can be assigned to a security profile. An existing default policy set is automatically assigned at system boot up.

2 Policy—A policy contains rules. A policy can contain rules that can be ordered. An existing default policy is automatically assigned at system boot up. The default policy has a default rule that has an action as **drop**.

3 Rule—A rule contains the conditions for regulating traffic. The default policy has a default rule that has an action as **drop**. Conditions for a rule can be set using the network, custom, and virtual machine attributes.

4 Object group—An object group object can be created under an organization node. It defines a collection of condition expressions on a specific system defined or on a custom attribute. An object group can be referred in a policy rule condition when a member or not-member operator is selected. The rule condition referring to the object group evaluates to true if any of the expressions in the object group evaluate to true.

5 Security Profile Dictionary—A Cisco VNMC security profile dictionary is a logical collection of security attributes. You define dictionary attributes for use in a security profile. A security profile dictionary is created at the root or tenant node. You can only create one dictionary for a tenant and only one dictionary for the root. The security profile dictionary allows the user to define names of custom attributes. Custom attribute values are specified on security profile objects. Custom attributes can be used to define policy rule conditions. Attributes configured in a root level dictionary can be used by any tenant. Creation of a dictionary below tenant level is not supported.

6 Zone—A zone defines a set of virtual machines based on conditions. The zone name is used in the authoring rules.

Security policies are created and then pushed to the Cisco VSG.

Configuring Security Profiles

Adding a Security Profile

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.

Step 2 In the **Navigation** pane, click the **Security Policies** subtab.

Step 3 In the **Navigation** pane, expand **root** > **Security Profiles**

Step 4 In the **Work** pane, click the **Add Security Profile** link.

Note You can add the component at any organizational level.

Step 5 In the **Add Security Profile** dialog box, **General** tab area, complete the following fields:

Name	Description
Name field	The name of the security profile. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.

Name	Description
Description field	A description of the security profile. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon. You cannot change this description after it is saved.
Policy Set drop-down list	A selectable drop-down list of policy sets.
Add Policy Set link	A link to add a policy set.
Resolved Policy Set field	A link to edit the resolved policy set.

Table 8: Resolved Policies Area

Name	Description
(Un)assign Policy link	The link to unassign a policy.
Name column	The name of the rule.
Source Condition column	Contains the source condition specified.
Destination Condition column	Contains the destination condition specified.
Protocol column	Contains the protocol specified.
Ethertype column	Contains the Ethertype specified.
Action column	Contains the action specified for the rule.
Description column	Contains a description for the rule.

Step 6 In the **Add Security Profile** dialog box, **Attributes** tab area, complete the following fields:

Name	Description
Add link	The link opens a dialog box where you can add an attribute.
Name column	The name of the attribute.
Value column	The attribute value.

Step 7 Click **OK**.

Editing a Security Profile

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Security Policies** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Security Profiles** .
Step 4 In the **Work** pane, click the security profile you want to edit.
Step 5 Click the **Edit** link.
Step 6 In the **Edit Security Profile** dialog box, **General** tab area, modify the following fields as appropriate:

Name	Description
Name field	The name of the security profile.
Description field	A user-defined description of the object.
Policy Set drop-down list	A selectable drop-down list of policy sets.
Resolved Policy Set field	A link to edit the resolved policy set.

Table 9: Resolved Policies Area

Name	Description
(Un)assigned Policy column	The link to a dialog box where you can assign or unassign policies.
Source Condition column	Contains the source condition specified.
Destination Condition column	Contains the destination condition specified.
Protocol column	Contains the protocol specified.
Ethertype column	Contains the Ethertype specified.
Action column	Contains the action specified for the rule.
Description column	A description of the component.

Step 7 In the **Edit Security Profile** dialog box, **Attributes** tab area, modify the following fields as appropriate:

Name	Description
Add link	Allows you to add a Security Profile attribute.
Name column	The name of the Security Profile attribute.
Value column	A value for the attribute.

Step 8 Click **OK**.

Deleting a Security Profile

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Security Policies** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Security Profiles**.
Step 4 In the **Work** pane, click the security profile you want to delete.
Step 5 Click the **Delete** link.
Step 6 In the **Confirm** dialog box, click **OK**.

Deleting a Security Profile Attribute

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Security Policies** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Security Profiles**.
Step 4 In the **Navigation** pane, click the security profile that contains the attribute you want to delete.
Step 5 In the **Work** pane, click the **Attributes** tab.
Step 6 Click the attribute you want to delete.
Step 7 Click the **Delete** link.
Step 8 In the **Confirm** dialog box, click **OK**.

Assigning a Policy

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Security Policies** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Security Profiles**.
Step 4 In the **Navigation** pane, click the profile where you want to assign the policy.
Step 5 In the **Work** pane, click the **(Un)assign Policy** link.
Step 6 In the **(Un)assign Policy** dialog box, move the policy you want assigned to the **Assigned** list.
Step 7 Click **OK**.

Unassigning a Policy

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Security Policies** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Security Profiles**.
Step 4 In the **Navigation** pane, click the profile where you want to unassign the policy.
Step 5 In the **Work** pane, click the **(Un)assign Policy** link.
Step 6 In the **(Un)assign Policy** dialog box, move the policy you want unassigned to the **Available** list.
Step 7 Click **OK**.

Configuring Security Policy Attributes

Configuring Object Groups

Adding an Object Group

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.

Step 2 In the **Navigation** pane, click the **Security Policies** subtab.

Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Object Groups**.

Step 4 In the **Work** pane, click the **Add Object Group** link.

Note You can add the component at any organizational level.

Step 5 In the **Add Object Group** dialog box, complete the following fields:

Name	Description
Name field	The name of the object group. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.
Description field	A description of the object group. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon. You cannot change this description after it is saved.
Attribute Type drop-down list	The attribute types available to select.
Attribute Name drop-down list	The attribute names available to select.
Add Attribute link	The link opens a dialog box where you can add an attribute.
Resolved Attribute field	The resolved attribute link.

Step 6 Click **OK**.

Adding an Object Group Expression

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.

Step 2 In the **Navigation** pane, click the **Security Policies** subtab.

Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Object Groups**.

Step 4 In the **Work** pane, click the **Add Object Group** link.

Note You can add the component at any organizational level.

Step 5 In the **Add Object Group** dialog box, click the **Add** link:

Step 6 In the **Add Object Group Expression** dialog box, complete the following fields:

Name	Description
Attribute Name field	The name of the attribute.
Operator drop-down list	The list of selectable operators.
Attribute Value field	The value of the attribute.

Step 7 Click **OK**.

Editing an Object Group

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.

Step 2 In the **Navigation** pane, click the **Security Policies** subtab.

Step 3 In the **Navigation** pane, expand**root** > **Advanced** > **Advanced** > **Object Groups**.

Step 4 In the **Work** pane, click the object group you want to edit.

Step 5 Click the **Edit** link.

Step 6 In the **Edit Object Group** dialog box **General** tab area, edit the appropriate fields:

Name	Description
Name field	The name of the object group. This field cannot be edited on this tab.

Name	Description
Description field	The description of the object group. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon. You cannot change this description after it is saved.
Attribute Type drop-down list	A list that contains attribute types.
Attribute Name drop-down list	A list that contains attribute names

Table 10: Expression Area

Name	Description
Operator column	The operator used.
Value column	The attribute value.

Step 7 Click **OK**.

Editing an Object Group Expression

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.

Step 2 In the **Navigation** pane, click the **Security Policies** subtab.

Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Object Groups** and click the object group where you want to edit an expression.

Step 4 In the **Work** pane, click the **Edit** link in the **Expression** area.

Step 5 In the **Expressions** area, click the expression you want to edit.

Step 6 In the **Edit Expression** dialog box modify the appropriate fields:

Name	Description
Attribute Name field	The name of the attribute.
Operator drop-down list	The list of selectable operators.
Attribute Value field	The value of the attribute.

Step 7 Click **OK**.

Deleting an Object Group

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Security Policies** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Object Groups**.
Step 4 In the **Navigation** pane, click the **Object Groups** node.
Step 5 In the **Work** pane, click the object group you want to delete.
Step 6 Click the **Delete** link.
Step 7 In the **Confirm** dialog box, click **Yes**.

Deleting an Object Group Expression

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Security Policies** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Object Groups**.
Step 4 In the **Navigation** pane, click the object group that contains the expression you want to delete.
Step 5 In the **Expression** area, click the expression you want to delete.
Step 6 Click the **Delete** link.
Step 7 In the **Confirm** dialog box, click **Yes**.

Configuring a Policy

Adding a Policy

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.

Step 2 In the **Navigation** pane, click the **Security Policies** subtab.

Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Policies**.

Step 4 In the **Work** pane, click the **Add Policy** link.

Step 5 In the **Add Policy** dialog box, complete the following fields:

Name	Description
Name	The name of the policy. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.
Description	The description of the policy. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon. You cannot change this description after it is saved.

Table 11: Rules Area

Name	Description
Add Rule link	Opens a dialog box that allows you to add a rule.
Up and **Down** arrows	Changes the priority of the selected policies.
Name column	Contains the rule names.
Source Condition column	Contains the source condition specified
Destination Condition column	Contains the destination condition specified
Protocol column	Contains the protocol specified
Ethertype column	Contains the EtherType specified
Action column	Contains the action specified for the rule.

Name	Description
Description column	Contains a description for the rule.

Step 6 Click **OK**.

Editing a Policy

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Security Policies** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Policies**.
Step 4 In the **Work** pane, click the policy you want to edit.
Step 5 Click the **Edit** link.
Step 6 In the **Edit Policy** dialog box, **General** tab area, modify the following fields as appropriate:

Name	Description
Name field	A component name.
Description field	A component description.

Table 12: Rules Area

Name	Description
Add Rule link	Opens a dialog box that allows you to add a rule.
Up and **Down** arrows	Changes the priority of the selected policies.
Name column	Contains the rule names.
Source Condition column	Contains the source condition specified
Destination Condition column	Contains the destination condition specified
Protocol column	Contains the protocol specified
Ethertype column	Contains the EtherType specified
Action column	Contains the action specified for the rule.

Name	Description
Description column	Contains a description for the rule.

Step 7 Click **Apply**, and then click **OK**.

Deleting a Rule-Based Policy

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Security Policies** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Policies**.
Step 4 In the **Work** pane, click the policy you want to delete.
Step 5 Click the **Delete** link.
Step 6 In the **Confirm** dialog box, click **Yes**.

Adding a Rule

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Security Policies** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Policies**.
Step 4 In the **Work** pane, click the **Add Policy** link.
Note You can add the component at any organizational level.
Step 5 In the **Add Policy** dialog box, click the **Add Rule** link.
Step 6 In the **Add Rule** dialog box, complete the following fields:

Name	Description
Name field	The name of the rule. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.

Name	Description
Description field	The description of the rule. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon. You cannot change this description after it is saved.
Action to Take area	The area in which you manage actions. • **drop** radio button—Click to set the action to drop. • **permit** radio button—Click to set the action to permit. • **reset** radio button—Click to set the action to reset. You can also check the **log** check box to enable logging.
Protocol area	The area in which you set the protocol. • **Any** check box—Check to use any protocol, and uncheck to choose a protocol. • **Operator** drop-down list—Choose an operator from the drop-down list. • **Value** drop-down list—Choose a protocol from the drop-down list.
Ether Type area	The area in which you set the Ethernet type. • **Any** check box—Check to use any value, and uncheck to enter a value. • **Operator** drop-down list—Choose an operator from the drop-down list. • **Value** field—Enter a hex number in the field.

Step 7 In the **Source Conditions** area, click the **Add** link to open the **Add Source Condition** dialog box, and choose the fields as appropriate:

Table 13: Source Conditions Area

Name	Description
Add link	Clicking the **Add** link opens the **Add Source Condition** dialog box.
Attribute Name column	The name of the attribute.
Operator column	The operator value specified.
Attribute Value column	The attribute value specified.

Step 8 In the **Destination Conditions** area, click the **Add** link to open the **Add Destination Condition** dialog box, and choose the fields as appropriate:

Table 14: Destination Conditions Area

Name	Description
Add link	Clicking the **Add** link opens the **Add Destination Condition** dialog box.
Attribute Name column	The name of the attribute.
Operator column	The operator value specified.
Attribute Value column	The attribute value specified.

Step 9 Click **OK**.

Editing a Rule

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Security Policies** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Policies** > ***Policy_name*** where you want to edit a rule.
Step 4 In the **Work** pane, click the *Rule_name* you want to edit.
Step 5 Click the **Edit** link.
Step 6 In the **Edit Rule** dialog box **General** tab area, modify the fields:
a) Modify the following fields as appropriate:

Name	Description
Name field	The name of the rule.
Description field	A description of the rule. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon. You cannot change this description after it is saved.
Action to Take area	The area in which you manage actions. • **drop** radio button—Click to set the action to drop. • **permit** radio button—Click to set the action to permit. • **reset** radio button—Click to set the action to reset. You can also check the **log** check box to enable logging.
Protocol area	The area in which you set the protocol. • **Any** check box—Check to use any protocol, and uncheck to choose a protocol. • **Operator** drop-down list—Choose an operator from the drop-down list. • **Value** drop-down list—Choose a protocol from the drop-down list.
Ether Type area	The area in which you set the Ethernet type. • **Any** check box—Check to use any value, and uncheck to enter a value. • **Operator** drop-down list—Choose an operator from the drop-down list. • **Value** field—Enter a hex number in the field.

b) In the **Source Conditions** area, modify the appropriate fields:

Table 15: Source Conditions Area

Name	Description
Add link	Clicking the **Add** link opens the **Add Source Condition** dialog box.
Attribute Name column	The name of the attribute.
Operator column	The operator value specified.
Attribute Value column	The attribute value specified.

c) In the **Destination Conditions** area, modify the appropriate fields:

Table 16: Destination Conditions Area

Name	Description
Add link	Clicking the **Add** link opens the **Add Destination Condition** dialog box.
Attribute Name column	The name of the attribute.
Operator column	The operator value specified.
Attribute Value column	The attribute value specified.

Step 7 Click **OK**.

Step 8 In the *Policy_name* dialog box, click **Save**.

Deleting a Rule

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Security Policies** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Policies**.
Step 4 In the **Work** pane, click the Policy where you want to delete a rule.
Step 5 Click the **Edit** link.
Step 6 In the **Edit Policy** dialog box, click the rule you want to delete.
Step 7 Click the **Delete** link.
Step 8 In the **Confirm** dialog box, click **Yes**.

Deleting a Source or a Destination Condition

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Security Policies** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Policies**.
In the **Navigation** pane, click the policy that contains the source or destination condition you want to delete.
Step 4 In the **Navigation** pane, click the policy that contains the source or destination condition you want to delete.
Step 5 In the **Work** pane, click the **Edit Rule** link.
Step 6 In the **Edit Rule** dialog box, click the source or a destination condition you want to delete.
Step 7 Click the **Delete** link in the associated area.
Step 8 In the **Confirm** dialog box, click **Yes**.

Configuring a Policy Set

Adding a Policy Set

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.

Step 2 In the **Navigation** pane, click the **Security Policies** subtab.

Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Policy Sets**.

Note You can add the component at any organizational level.

Step 4 In the **Work** pane, click the **Add Policy Set** link.

Step 5 In the **Add Policy Set** dialog box, **General** tab area, complete the following fields, and optionally, move policies between the **Available** and **Assigned** areas:

Name	Description
Name field	A name for the component. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.
Description field	A user-defined description of the component. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon. You cannot change this description after it is saved.

Table 17: Policies Area

Name	Description
Add Policy link	Opens a dialog box that allows you to add a policy.
Up and **Down** arrows	Changes the priority of the selected policies.
Available column	Lists the policies created and available. Use arrows between the columns to move policies to the **Assigned** column.
Assigned column	Lists the policies assigned to the policy set. Use arrows between the columns to move policies to the **Available** column.

Step 6 In the **Add Policy Set** dialog box, click **OK**.

Editing a Policy Set

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Security Policies** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Policy Sets**.
Step 4 In the **Work** pane, click the policy set you want to edit.
Step 5 Click the **Edit** link.
Step 6 In the **Edit Policy Set** dialog box, **General** tab area, modify the following fields as appropriate:

Name	Description
Name field	A name for the component.
Description field	A user-defined description of the component.

Table 18: Policies Area

Name	Description
Add Policy link	Opens a dialog box that allows you to add a policy.
Up and **Down** arrows	Changes the priority of the selected policies.
Available column	Lists the policies created and available. Use arrows between the columns to move policies to the **Assigned** column.
Assigned column	Lists the policies assigned to the policy set. Use arrows between the columns to move policies to the **Available** column.

Step 7 Click **OK**.

Deleting a Policy Set

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Security Policies** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Policy Sets**.
Step 4 In the **Work** pane, click the policy set you want to delete.
Step 5 Click the **Delete** link.
Step 6 In the **Confirm** dialog box, click **Yes**.

Configuring Zones

Adding a vZone

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Security Policies** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced**.
Step 4 In the **Navigation** pane, click the **vZones** node.
Note You can add the component at any organizational level.
Step 5 In the **Work** pane, click the **Add vZone** link.
Step 6 In the **Add vZone** dialog box, complete the following fields:

Name	Description
Name field	The name of the vZone. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.
Description field	The description of the vZone. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon. You cannot change this description after it is saved.

Step 7 Click the **Add** link in the **vZone Condition** area and complete the following tasks:

a) In the Add vZone Condition dialog box, complete the following areas:

Name	Description
Attribute Type drop-down list	A list of attribute types. It can be one of the following attributes: • **Network** • **VM** • **User Defined**

Table 19: Expression Area

Name	Description
Attribute Name	The attribute name. Depending upon the attribute type selected, a different set of choices are available.
Operator	The operator used. Depending upon the attribute type selected, a different set of choices are available.
Attribute Value	The attribute value. Depending upon the attribute type selected, a different set of choices is available.

b) Click **OK**.

Step 8 In the **Add vZone** dialog box, click **OK**.

Editing a vZone

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.

Step 2 In the **Navigation** pane, click the **Security Policies** subtab.

Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **vZones** node.

Step 4 In the **Navigation** pane, click the **vZones** node.

Step 5 In the **Work** pane, click the vzone you want to edit.

Step 6 Click the **Edit** link.

Step 7 In the **Edit Zone** dialog box **General** tab area, change the appropriate fields:

Name	Description
Name column	A list of components.
Description column	A list of component descriptions.

Step 8 In the **Edit Zone** dialog box **vZone Conditions** area, do the following:

a) Click an attribute you want to edit.

b) Click the **Edit** link to open the **Edit Condition** dialog box, and make the appropriate changes in the following fields:

Name	Description
Attribute Type drop-down list	The list you use to manage attribute types.

Table 20: Expression area

Name	Description
Attribute Name drop-down list	Contains attribute names.
Operator drop-down list	Contains operators.
Attribute Value field	Contains attribute values.

c) Click **OK**.

Step 9 In the **Edit vZone** dialog box, click **OK**.

Deleting a vZone

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.

Step 2 In the **Navigation** pane, click the **Security Policies** subtab.

Step 3 In the **Navigation** pane, expand **root** > **Advanced**.

Step 4 In the **Navigation** pane, click the **vZones** node.

Step 5 In the **Work** pane, click the vZone you want to delete.

Step 6 Click the **Delete** link.

Step 7 In the **Confirm** dialog box, click **Yes**.

Deleting a vZone Condition

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Security Policies** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **vZones** .
Step 4 In the **Navigation** pane, click the vZone that contains the condition you want to delete.
Step 5 In the **Work** pane, click the **Edit** link.
Step 6 In the **Edit vZone** dialog box, **vZone Condition** area, click the condition you want to delete.
Step 7 Click the **Delete** link.
Step 8 In the **Confirm** dialog box, click **Yes**.
Step 9 In the **Edit vZone** dialog box, click **Apply**.

Configuring Security Profile Dictionary

Adding a Security Profile Dictionary

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Security Policies** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Security Profile Dictionary** node.
Step 4 In the **Work** pane, click the **Add Security Profile Dictionary** link.
Note You can create a security profile dictionary at the root or Tenant level.
Step 5 In the **Add Security Profile Dictionary** dialog box, complete the following fields as appropriate:

Name	Description
Name field	The name of the security profile. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.

Name	Description
Description field	A description of the security profile. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon. You cannot change this description after it is saved.
Policy Set drop-down list	A selectable drop-down list of policy sets.
Add Policy Set link	A link to add a policy set.
Resolved Policy Set field	A link to edit the resolved policy set.

Step 6 Click **OK**.

Adding a Security Profile Dictionary Attribute

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.

Step 2 In the **Navigation** pane, click the **Security Policies** subtab.

Step 3 In the **Navigation** pane, expand**root** > **Advanced** > **Security Profile Dictionary** to view and select the appropriate ***Security Profile Dictionary_name***.

Step 4 In the **Work** pane, click the **Edit** link to open the **Edit Security Profile Dictionary** dialog box.

Step 5 In the **Edit Security Profile Dictionary** dialog box, click the **Add Attribute** link.

Step 6 In the **Add Attribute** dialog box, complete the following fields:

Name	Description
Name field	The name of the **Security Profile Dictionary** attribute. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.
Description field	A description of the **Security Profile Dictionary** attribute. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon. You cannot change this description after it is saved.

Step 7 Click **OK**.

Editing a Security Profile Dictionary

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Security Policies** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Security Profile Dictionary**.
Step 4 In the **Work** pane, click the security profile dictionary you want to edit.
Step 5 Click the **Edit** link.
Step 6 In the **Edit Security Profile Dictionary** dialog box, modify the fields as appropriate:

Name	Description
Name field	The name of the security profile dictionary. You cannot edit this field.
Description field	A description of the security profile dictionary.

Step 7 Click **OK**.

Editing a Security Profile Dictionary Attribute

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Security Policies** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Security Profile Dictionary** node.
Step 4 In the **Work** pane, click the security profile dictionary that contains the attribute you want to edit.
Step 5 Click the **Edit** link.
Step 6 In the **Edit Security Profile Dictionary** dialog box, **Attributes** area, click the attribute you want to edit.
Step 7 Click the **Edit** link.
Step 8 In the **Edit Attribute** dialog box, modify the following fields as appropriate:

Name	Description
Name field	The name of the security profile dictionary attribute.
Description field	A description of the security profile dictionary attribute.

Step 9 Click **OK**.

Step 10 In the **Edit Security Profile Dictionary** dialog box, click **OK**.

Deleting a Security Profile Dictionary

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.

Step 2 In the **Navigation** pane, click the **Security Policies** subtab.

Step 3 In the **Navigation** pane, expand**root** > **Advanced** > **Security Profile Dictionary** node.

Step 4 In the **Work** pane, click the security profile dictionary you want to delete.

Step 5 Click the **Delete** link.

Step 6 In the **Confirm** dialog box, click **OK**.

Deleting a Security Profile Dictionary Attribute

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.

Step 2 In the **Navigation** pane, click the **Security Policies** subtab.

Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Security Profile Dictionary**.
In the **Navigation** pane, click the dictionary that contains the attribute you want to delete.

Step 4 In the **Work** pane, click the **Edit** link.

Step 5 In the **Edit Security Profile Dictionary** dialog box, **Attributes** area, click the attribute you want to delete.

Step 6 Click the **Delete** link.

Step 7 In the **Confirm** dialog box, click **OK**.

CHAPTER 10

Configuring Device Profiles and Policies

This chapter includes the following sections:

Device Configuration

Cisco VNMC provides the option to configure devices. You configure devices by adding policies to device profile. You can add DNS and NTP server policies, SNMP policies, and syslog, fault, core and log file policies. You can also enable policy engine logging for the device.

Device Profiles

Device profiles specify device configuration policies that are applied on a per device basis. You create and delete device profiles on the **Device Configurations** tab.

You create device profiles for the Cisco VSG. Policies that reside at the current level or higher are available for assignment to a profile. If an assigned policy does not exist, the default policy is automatically assigned. Policies can be assigned to a device profile under the **Policies** tab when creating the device profile. While creating or editing device profiles, you also have the option of creating policies in the same dialog boxes.

Device Policies

Device policies that can be created and assigned to a device profile are as follows:

- Core file policy
- Fault policy
- Logging policy
- SNMP policy

- Syslog policy

DNS server, NTP server and domain names can be assigned as inline policies. A time zone setting can also be assigned to the profile.

When the system boots up, the fault, logging, SNMP, and syslog policies already have existing default policies. The default policies cannot be deleted but may be modified. A device profile uses name resolution to resolve policy assignments. For details, see Name Resolution in a Multi-tenancy Environment, on page 74

Device policies capture the device level configuration objects that can be applied to one of more VSGs. The following policies created under root only, in the Device Policies area, will be visible in the VNMC profile:

- Core file policy
- Fault policy
- Logging policy
- Syslog policy

Policies created under root are visible to both the VNMC profile and the Device profile.

Configuring Device Profiles

Adding a Firewall Device Profile

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.

Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.

Step 3 In the **Navigation** pane, expand **root** > **Device Profiles** node.

Note You can add the component at any organizational level.

Step 4 In the **Work** pane, click the **Add Firewall Device Profile** link.

Step 5 In the **Add Firewall Device Profile** dialog box, **General** tab area, complete the following fields:

Name	Description
Name field	The name of the profile. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.
Description field	A description of the profile. The description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.

Name	Description
Time Zone drop-down list	A list of time zones. Use the list to designate a time zone.

Step 6 In the **Add Firewall Device Profile** dialog box, click the **Policies** tab.

a) In the **DNS Servers** area, complete the following fields as appropriate:

Name	Description
Add DNS Server link	Opens a dialog box that allows you to specify a new DNS server.
Delete link	Deletes the DNS server IP address selected in the **IP Address** table.
Up and **Down** arrows	Changes the priority of the selected DNS Server IP address.
IP Address table	Contains the IP addresses for the DNS servers configured in the system. VNMC uses the DNS servers in the order they appear in the table.

b) In the **NTP Servers** area, complete the following fields as appropriate:

Name	Description
Add NTP Server link	Opens a dialog box that allows you to specify a new NTP server.
Delete link	Deletes the NTP server hostname selected in the **Hostname** table.
Up and **Down** arrows	Changes the priority of the selected NTP Server hostname.
Hostname table	Contains the NTP server hostnames configured in the system. VNMC uses the NTP server hostnames in the order they appear in the table.

c) In the **DNS Domains** area, complete the following fields as appropriate:

Name	Description
Add link	Opens a dialog box to specify a new DNS domain name.
Edit link	Edits the DNS domain name selected in the **DNS Domains** table. The **default** DNS name cannot be edited.
Delete link	Deletes the DNS domain name selected in the **DNS Domains** table.
DNS Domains table	Contains the default DNS domain name and domain in the system.

d) In the Policies area, complete the following fields as appropriate:

Name	Description
SNMP area	The SNMP policies associated with this profile can be selected, added, or edited. Contains the **Resolved Policy** field.
Syslog area	The syslog policies associated with this profile can be selected, added, or edited. Contains the **Resolved Policy** field.
Fault area	The fault policies associated with this profile can be selected, added, or edited. Contains the **Resolved Policy** field.
Core File area	The core file policies associated with this profile can be selected, added, or edited. Contains the **Resolved Policy** field.
Policy Agent Log File area	The policy agent log file policies associated with this profile can be selected, added, or edited. Contains the **Resolved Policy** field.
Policy Engine Logging area	• **enabled** radio button enables logging. • **disabled** radio button disables logging.

Step 7 In the **Add Firewall Device Profile** dialog box, click **OK**.

Editing a Firewall Device Profile

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.

Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.

Step 3 In the **Navigation** pane, expand **root**.

Step 4 In the **Navigation** pane, click the **Device Profiles** node.

Step 5 In the **Work** pane, click the profile you want to edit.

Step 6 Click the **Edit** link.

Step 7 In the **Edit** dialog box **General** tab area, modify the following fields as appropriate:

Name	Description
Name field	The name of the profile. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.
Description field	A description of the profile. The description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.
Time Zone drop-down list	A list of time zones. Use the list to designate a time zone.

Step 8 In the **Add Firewall Device Profile** dialog box, click the **Policies** tab.

a) In the **DNS Servers** area, modify the following fields as appropriate:

Name	Description
Add DNS Server link	Opens a dialog box that allows you to specify a new DNS server.
Delete link	Deletes the DNS server IP address selected in the **IP Address** table.
Up and **Down** arrows	Changes the priority of the selected DNS Server IP address.

Name	Description
IP Address table	Contains the IP addresses for the DNS servers configured in the system. VNMC uses the DNS servers in the order they appear in the table.

b) In the **NTP Servers** area, modify the following fields as appropriate:

Name	Description
Add NTP Server link	Opens a dialog box that allows you to specify a new NTP server.
Delete link	Deletes the NTP server hostname selected in the **Hostname** table.
Up and **Down** arrows	Changes the priority of the selected NTP Server hostname.
Hostname table	Contains the NTP server hostnames configured in the system. VNMC uses the NTP server hostnames in the order they appear in the table.

c) In the **DNS Domains** area, modify the following fields as appropriate:

Name	Description
Add link	Opens a dialog box to specify a new DNS domain name.
Edit link	Edits the DNS domain name selected in the **DNS Domains** table. The **default** DNS name cannot be edited.
Delete link	Deletes the DNS domain name selected in the **DNS Domains** table.
DNS Domains table	Contains the default DNS domain name and domain in the system.

d) In the Policies area, modify the following fields as appropriate:

Name	Description
SNMP area	The SNMP policies associated with this profile can be selected, added, or edited. Contains the **Resolved Policy** field.
Syslog area	The syslog policies associated with this profile can be selected, added, or edited. Contains the **Resolved Policy** field.
Fault area	The fault policies associated with this profile can be selected, added, or edited. Contains the **Resolved Policy** field.
Core File area	The core file policies associated with this profile can be selected, added, or edited. Contains the **Resolved Policy** field.
Policy Agent Log File area	The policy agent log file policies associated with this profile can be selected, added, or edited. Contains the **Resolved Policy** field.
Policy Engine Logging area	• **enabled** radio button enables logging. • **disabled** radio button disables logging.

Step 9 Click **OK**.

Deleting a Firewall Device Profile

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Device Profiles**.
Step 4 In the **Navigation** pane, click the **Device Profiles** node.
Step 5 In the **Work** pane, click the device profile you want to delete.
Step 6 Click the **Delete** link.
Step 7 In the **Confirm** dialog box, click **OK**.

Configuring Device Policies

Configuring Core Policy

Adding a Core File Policy for a Device Profile

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.

Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.

Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies**.

Step 4 In the **Navigation** pane, click the **Core File** node.

Step 5 In the **Work** pane, click the **Add Core File Policy** link.

Note You can add the policy at any organizational level.

Step 6 In the **Add Core File Policy** dialog box, complete the following fields:

Name	Description
Name field	The name of the core file policy. This name can be between 1 and 511 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been created.
Description field	The description of the core file policy. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon. You cannot change this description after it is saved.
Admin State drop-down list	The state of the core file policy. It can be one of the following states: • **Enabled**—Enables the core file policy. TFTP is used. • **Disabled**—Disables the core file policy.
Hostname field	The hostname or IP address to connect using TFTP. **Note** If you use a hostname rather than an IP address, you must configure a DNS server in Cisco VNMC.

Name	Description
Port field	The port number to send the core dump file to.
Protocol field	The protocol used to export the core dump file. This field cannot be edited.
Path field	The path to use when storing the core dump file on a remote system. The default path is /tftpboot. An example path would be /tftpboot/test, where test is the sub-folder.

Step 7 Click **OK**.

Editing a Core File Policy for a Device Profile

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies**.
Step 4 In the **Navigation** pane, click the **Core File** node.
Step 5 In the **Work** pane, click the **General** tab.
Step 6 On the **General** tab, click the core file policy you want to edit.
Step 7 On the **General** tab click the **Edit** link.
Step 8 In the **Edit** dialog box, modify the following fields as appropriate:

Name	Description
Name field	The name of the core file policy.
Description field	A description of the core file policy.
Admin State drop-down list	A list of administrative states. This can be one of the following states: • **enabled**—Enables the core file policy. • **disabled**—Disables the core file policy.
Hostname field	The hostname or IP address. **Note** If you use a hostname rather than an IP address, you must configure a DNS server.

Name	Description
Port field	The port number used when exporting the core dump file. The default path is /tftpboot. To mention a sub folder under tftpboot, use, for example, /tftpboot/test.
Protocol field	The protocol used to export the core dump file.
Path check box	The path to use when storing the core dump file on the remote system.

Step 9 Click **OK**.

Deleting a Core File Policy for a Device Profile

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies**.
Step 4 In the **Navigation** pane, click the **Core File** node.
Step 5 In the **Work** pane, click on the core file you want to delete.
Step 6 Click the **Delete** link.
Step 7 In the **Confirm** dialog box, click **Yes**.

Configuring Fault Policies

Adding a Fault Policy for a Device Profile

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Device Policies**.
Step 4 In the **Work** pane, click the **Add Fault Policy** link.
Note You can add the policy at any organizational level.

Step 5 In the **Add Fault Policy** dialog box, complete the following fields:

Name	Description
Name field	A user-defined name for the fault policy. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.
Description field	A user-defined description of the fault policy.
Flapping Interval spinbox	Flapping occurs when a fault is raised and cleared several times in rapid succession. To prevent this, the system does not allow a fault to change its state until this amount of time has elapsed since the last state change. If the condition reoccurs during the flapping interval, the fault returns to the active state. If the condition does not reoccur during the flapping interval, the fault is cleared. What happens at that point depends on the setting in the **Clear Faults Retention Action** field. The number of hours, minutes, and seconds that should pass before the system allows a fault to change its state. The default flapping interval is 10 seconds.
Clear Faults Retention Action drop-down list	The state of the clear faults retention action. It can be one of the following states: • **retain**—Retains the cleared faults section. • **delete**—The system immediately deletes all fault messages as soon as they are marked as cleared.
Clear Faults Retention Interval radio-button	The state of the clear faults retention interval. It can be one of the following states: • **Forever**—The system leaves all cleared fault messages regardless of how long they have been in the system. • **Other**—The system displays the **dd:hh:mm:ss** spinbox for selection of the number of days, hours, minutes, and seconds that should pass before the system deletes a cleared fault message. The default retention interval is 1 hour.

Step 6 Click **OK**.

Editing a Fault Policy for a Device Profile

Note When the system boots up, a default policy already exists. The default policy cannot be deleted but may be modified.

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.

Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.

Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies.**.

Step 4 In the **Navigation** pane, click the **Fault** node.

Step 5 In the **Work** pane, click the fault policy you want to edit.

Step 6 Click the **Edit** link.

Step 7 In the **Edit** dialog box, modify the following fields as appropriate:

Name	Description
Name field	The name of the fault policy.
Description field	A description of the fault policy.
Flapping Interval spinbox	The spinbox that lists flapping intervals. Use the box to set the interval. Flapping occurs when a fault is raised and cleared several times in rapid succession. To prevent this, the system does not allow a fault to change its state until this amount of time has elapsed since the last state change. The interval is the number of hours, minutes, and seconds that should pass before the system allows a fault to change its state. If the condition reoccurs during the flapping interval, the fault returns to the active state. If the condition does not reoccur during the flapping interval, the fault is cleared. What happens at that point depends on the setting in the **Clear Faults Retention Action** field. The default flapping interval is 10 seconds.

Name	Description
Clear Faults Retention Action drop-down list	The list that contains fault retention actions. Use the list to set an action. This can be one of the following actions: • **retain**—The system retains fault messages. • **delete**—The system immediately deletes all fault messages as soon as they are marked as cleared.
Clear Faults Retention Interval radio-button	The control that sets the retention interval. Use the control to set the interval. This can be one of the following values: • **forever**—The system leaves all cleared fault messages regardless of how long they have been in the system. • **other**—The system displays the **dd:hh:mm:ss** spinbox for selection of the number of days, hours, minutes, and seconds that should pass before the system deletes a cleared fault message. The default retention interval is 1 hour.

Step 8 Click **OK**.

Deleting a Fault Policy for a Device Profile

Note When the system boots up, a default policy already exists. The default policy cannot be deleted but may be modified.

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies**.
Step 4 In the **Navigation** pane, click the **Fault** node.
Step 5 In the **Work** pane, click the fault you want to delete.
Step 6 Click the **Delete** link.
Step 7 In the **Confirm** dialog box, click **OK**.

Configuring Log File Policies

Adding a Logging Policy for a Device Profile

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies**.
Step 4 In the **Navigation** pane, click the **Log File** node.
Note You can add the policy at any organizational level.
Step 5 In the **Work** pane, click the **Add Logging Policy** link.
Step 6 In the **Add Logging Policy** dialog box, complete the following fields:

Name	Description
Name field	The name of the logging policy. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.
Description field	A description of the logging policy.

Name	Description
Log Level drop-down list	A list of logging severity levels. This can be one of the following levels: • **debug0** • **debug1** • **debug2** • **debug3** • **debug4** • **info** • **warn** • **minor** • **major** • **crit** The default log level is **info**.
Backup Files Count field	The number of backup files that are filled before they are overwritten. The range is 1 to 9 files. The default is 2 files.
File Size (bytes) field	The backup file size. The range is 1MB to 100MB. The default file size is 5MB.

Step 7 Click **OK**.

Editing a Logging Policy for a Device Profile

Note When the system boots up, a default policy already exists. The default policy cannot be deleted but may be modified.

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.

Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.

Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies**.

Step 4 In the **Navigation** pane, click the **Log File** node.

Step 5 On the **Work** pane, click the logging policy you want to edit.

Step 6 Click the **Edit** link.

Step 7 In the **Edit** dialog box, modify the appropriate fields:

Name	Description
Name field	The name of the logging policy. This field cannot be edited.
Description field	A description of the logging policy.
Log Level drop-down list	A list of logging levels. This can be one of the following levels: • **debug0** • **debug1** • **debug2** • **debug3** • **debug4** • **info** • **warn** • **minor** • **major** • **crit** The default log level is **info**.
Backup Files Count field	The number of backup files that are filled before they are overwritten. The range is 1 to 9 files. The default is 2 files.
File Size (bytes) field	The backup file size. The range is 1MB to 100MB. The default file size is 5MB.

Step 8 Click **OK**.

Deleting a Logging Policy for a Device Profile

Note When the system boots up, a default policy already exists. The default policy cannot be deleted but may be modified.

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.
Step 3 In the **Navigation** pane, expand the nodes **root** > **Advanced** > **Device Policies**.
Step 4 In the Navigation pane, click the **Log File** node.
Step 5 In the **Work** pane, click the logging policy you want to delete.
Step 6 Click the **Delete** link.
Step 7 In the **Confirm** dialog box, click **OK**.

Configuring SNMP Policies

Adding an SNMP Policy

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies**.
Step 4 In the **Navigation** pane, click the **SNMP** node.
Note You can add the policy at any organizational level.
Step 5 In the **Work** pane, click the **Add SNMP** link.
Step 6 In the **Add SNMP** dialog box, **General** tab area, complete the following fields as appropriate:

Table 21: General Tab

Name	Description
Name field	The name of the SNMP policy. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.
Description field	A description of the SNMP policy. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon. You cannot change this description after it is saved.
Admin State drop-down list	The administrative state of the policy. It can be one of the following states: • **enabled** • **disabled** The default state is enabled.
Location field	The physical location of the device.
Contact field	The contact person for the device.
SNMP Port field	The port where the SNMP agent is listening for requests. You cannot edit this field.

Step 7 In the **Add SNMP** dialog box, **Communities** tab area do the following:

a) Click the **Add SNMP Community** link.

b) In the **Add SNMP Community** dialog box, complete the following fields as appropriate:

Name	Description
Community field	The name of the community.
Role field	The role associated with the community string. You cannot edit this field.

c) Click **OK**.

Step 8 In the **Add SNMP** dialog box, click **OK**.

Editing an SNMP Policy

Note When the system boots up, a default policy already exists. The default policy cannot be deleted but may be modified.

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.

Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.

Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies**.

Step 4 Click the **SNMP** node where you want to edit an SNMP policy.

Step 5 In the **Work** pane, click the SNMP policy you want to edit.

Step 6 Click the **Edit** link.

a) In the **Edit SNMP** dialog box **General** tab area, edit the appropriate information:

Name	Description
Name field	The name of the SNMP policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been created.
Description field	A description of the SNMP policy.
Admin State drop-down list	The administrative state of the policy. It can be one of the following states: • **enabled** • **disabled** The default state is enabled.
Location field	The physical location of the device.
Contact field	The contact person for the device.
SNMP Port field	The port where the SNMP agent is listening for requests.

b) In the **Edit SNMP** dialog box **Communities** tab area, edit the information as appropriate:

Name	Description
Community column	The name of the community.
Role column	The role associated with the community string.

Note Depending upon the object you select in the table, different options will appear in the area above the table.

c) In the **Edit SNMP** dialog box **Trap** tab area, edit the information as appropriate:

Name	Description
Hostname field	The IP address of the SNMP host.
Port field	The port where the SNMP agent is listening for requests.
Community field	The name of the community.

d) In the **Edit SNMP Trap** dialog box, click **OK**.

Step 7 Click **OK**.

Deleting an SNMP Policy

Note When the system boots up, a default policy already exists. The default policy cannot be deleted but may be modified.

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies**.
Step 4 In the **Navigation** pane, click the **SNMP** node.
Step 5 In the **Work** pane, click the SNMP policy you want to delete.
Step 6 Click the **Delete** link.
Step 7 In the **Confirm** dialog box, click **Yes**.

Adding an SNMP Trap Receiver

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies**.
Step 4 In the **Navigation** pane, click the **SNMP** node.
Step 5 In the **Work** pane, click the **Add SNMP** link.
Step 6 Click the **Traps** tab.
Step 7 In the **Add SNMP** dialog box, click the **Add SNMP Trap** link.
Step 8 In the **Add SNMP Trap** dialog box, complete the following fields:

Name	Description
Hostname field	The IP address of the SNMP host.
Port field	The port where the SNMP agent is listening for requests. The default port is 162.
Community field	The name of the community.

Step 9 Click **OK**.

Editing an SNMP Trap Receiver

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies**.
Step 4 Click the **SNMP** > ***SNMP Policy_name*** where you want to edit the SNMP trap.
Step 5 In the **Work** pane, **Traps** tab area, click the hostname to edit.
Step 6 Click the **Edit** link.
Step 7 In the **Edit SNMP Trap** dialog box, edit the appropriate fields:

Name	Description
Hostname field	The IP address of the SNMP host.

Name	Description
Port field	The port where the SNMP agent is listening for requests.
Community field	The name of the community.

Step 8 Click **OK**.

Deleting an SNMP Trap Receiver

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies** > **SNMP**.
Step 4 In the **Navigation** pane, click the SNMP policy that contains the trap you want to delete.
Step 5 In the **Work** pane, click the **Traps** tab.
Step 6 In the **Work** pane, click the trap you want to delete.
Step 7 Click the **Delete** link.
Step 8 In the **Confirm** dialog box, click **Yes**.

Configuring Syslog Policies

Adding a Syslog Policy for a Device Profile

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies**.
Step 4 In the **Navigation** pane, click the **Syslog** node.
Note You can add the policy at any organizational level.
Step 5 In the **Work** pane, click the **Add Syslog** link.
Step 6 In the **Add Syslog** dialog box, complete the following tasks:

a) In the **Add Syslog** dialog box, **General** tab area, complete the following fields:

Table 22: General Tab

Name	Description
Name field	The name of the syslog policy. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.
Description field	The description of the syslog policy.
Port field	The TCP or UDP port where syslog messages are sent. You cannot edit this field.

b) In the **Add Syslog** dialog box, **Local Destinations** tab, complete the following fields:

Table 23: Console Area

Name	Description
Admin State radio button	The administrative state of the policy. It can be one of the following states: • **enabled** • **disabled**
Level radio button	The message level. It can be one of the following levels: • **alerts** • **critical** • **emergencies** If the **Admin State** is enabled, select the lowest message level that you want displayed. The system displays that level and above on the console.

Table 24: Monitor Area

Name	Description
Admin State radio button	The administrative state of the policy. It can be one of the following states: • **enabled** • **disabled**
Level drop-down list	The message levels. It can be one of the following levels: • **emergencies (0)** • **alerts (1)** • **critical (2)** • **errors (3)** • **warnings (4)** • **notifications (5)** • **information (6)** • **debugging (7)** If the **Admin State** is enabled, select the lowest message level that you want displayed. The system displays that level and above on the console.

Table 25: File Area

Name	Description
Admin State radio button	The administrative state of the policy. It can be one of the following states: • **enabled** • **disabled**

Name	Description
Level drop-down list	The message levels. It can be one of the following levels: • **emergencies (0)** • **alerts (1)** • **critical (2)** • **errors (3)** • **warnings (4)** • **notifications (5)** • **information (6)** • **debugging (7)** If the **Admin State** is enabled, select the lowest message level that you want displayed. The system displays that level and above on the console.
File Name field	The name of the file in which messages are logged.
Size (Bytes) field	The maximum size, in bytes, the file can be before the system begins to over-write messages.

Step 7 Click **OK**.

Editing a Syslog Policy for a Device Profile

Note When the system boots up, a default policy already exists. The default policy cannot be deleted but may be modified.

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.

Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.

Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies**.

Step 4 In the **Navigation** pane, click the **Syslog** node.

Step 5 In the **Work** pane, click the syslog policy you want to edit.

Step 6 Click the **Edit** link.

Step 7 In the **Edit Syslog** dialog box, modify the following fields as appropriate:

a) In the **Add Syslog** dialog box, **General** tab area, edit the following fields as appropriate:

Name	Description
Name field	The name of the syslog policy. This field cannot be edited.
Description field	The description of the syslog policy.
Port field	The TCP or UDP port where syslog messages are sent.

b) In the **Add Syslog** dialog box, **Local Destinations** tab, edit the following fields as appropriate:

Table 26: Console Area

Name	Description
Admin State radio button	The administrative state of the policy. It can be one of the following states: • **enabled** • **disabled**
Level radio button	The message level. It can be one of the following levels: • **alerts** • **critical** • **emergencies** If the **Admin State** is enabled, select the lowest message level that you want displayed. The system displays that level and above on the console.

Table 27: Monitor Area

Name	Description
Admin State radio button	The administrative state of the policy. It can be one of the following states: • **enabled** • **disabled**
Level drop-down list	The message levels. It can be one of the following levels: • **emergencies (0)** • **alerts (1)** • **critical (2)** • **errors (3)** • **warnings (4)** • **notifications (5)** • **information (6)** • **debugging (7)** If the **Admin State** is enabled, select the lowest message level that you want displayed. The system displays that level and above on the console.

Table 28: File Area

Name	Description
Admin State radio button	The administrative state of the policy. It can be one of the following states: • **enabled** • **disabled**

Name	Description
Level drop-down list	The message levels. It can be one of the following levels: • **emergencies (0)** • **alerts (1)** • **critical (2)** • **errors (3)** • **warnings (4)** • **notifications (5)** • **information (6)** • **debugging (7)** If the **Admin State** is enabled, select the lowest message level that you want displayed. The system displays that level and above on the console.
File Name field	The name of the file in which messages are logged.
Size (Bytes) field	The maximum size, in bytes, the file can be before the system begins to over-write messages.

Step 8 Click **OK**.

Deleting a Syslog Policy for a Device Profile

Note When the system boots up, a default policy already exists. The default policy cannot be deleted but may be modified.

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies**.
Step 4 In the **Navigation** pane, click the **Syslog** node.
Step 5 In the **Work** pane, click the syslog policy you want to delete.
Step 6 Click the **Delete** link.
Step 7 In the **Confirm** dialog box, click **Yes**.

Adding a Syslog Server for a Device Profile

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies** > **Syslog**.
Step 4 In the **Work** pane, click the syslog policy where you want to add the server.
Step 5 Click the **Add Syslog** link.
Step 6 In the Work pane, click the **Servers** tab.
Step 7 In the **Add Syslog** dialog box, click the **Add Syslog Server** link.
Step 8 In the **Add Syslog Server** dialog box, complete the following fields:

Name	Description
Server Type field	The type of server. It can be one of the following types: • **primary** • **secondary** • **tertiary**
Hostname/IP address field	The hostname or IP address where the syslog file resides.

Name	Description
Severity field	The severity level. It can be one of the following levels: • **emergencies (0)** • **alerts (1)** • **critical (2)** • **errors (3)** • **warnings (4)** • **notifications (5)** • **information (6)** • **debugging (7)**
Forwarding Facility field	The forwarding facility. It can be one of the following types: • **auth** • **authpriv** • **cron** • **daemon** • **ftp** • **kernel** • **local0** • **local1** • **local2** • **local3** • **local4** • **local5** • **local6** • **lpr** • **mail** • **news** • **syslog** • **user** • **uucp**

Name	Description
Admin State field	The administrative state of the policy. It can be one of the following states: • **enabled** • **disabled**

Step 9 Click **OK**.

Editing a Syslog Server for a Device Profile

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.

Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.

Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies** > **Syslog** node.

Step 4 In the **Work** pane, click the appropriate syslog where you want to edit a syslog server.

Step 5 Click the **Edit** link.

Step 6 In the **Edit Syslog** dialog box **Servers** tab area, click the syslog server you want to edit and click the **Edit** link.

Step 7 In the **Edit Syslog Server** dialog box modify the fields as appropriate.

Name	Description
Server Type field	The type of server. It can be one of the following types: • **primary** • **secondary** • **tertiary**
Hostname/IP address field	The hostname or IP address where the syslog file resides.

Name	Description
Severity field	The severity level. It can be one of the following levels: • **emergencies (0)** • **alerts (1)** • **critical (2)** • **errors (3)** • **warnings (4)** • **notifications (5)** • **information (6)** • **debugging (7)**
Forwarding Facility field	The forwarding facility. It can be one of the following types: • **auth** • **authpriv** • **cron** • **daemon** • **ftp** • **kernel** • **local0** • **local1** • **local2** • **local3** • **local4** • **local5** • **local6** • **lpr** • **mail** • **news** • **syslog** • **user** • **uucp**

Name	Description
Admin State field	The administrative state of the policy. It can be one of the following states: • **enabled** • **disabled**

Step 8 Click **OK**.

Deleting a Syslog Server for a Device Profile

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies** > **Syslog** node.
Step 4 In the **Work** pane, click the **Add Syslog** link.
Step 5 In the **Add Syslog** dialog box, click the **Servers** tab.
Step 6 Click the server you want to delete.
Step 7 Click the **Delete** link.
Step 8 In the **Confirm** dialog box, click **Yes**.

CHAPTER 11

Configuring Managed Resources

This chapter includes the following sections:

Managed Resources

Resource Management

The **Resource Management** tab displays Cisco VNMC resources to view and to manage. It displays and manages the following resources:

- Virtual Machines (VM)
- Virtual Security Gateways (Cisco VSG)
- Virtual Supervisor Modules (Nexus 1000V VSM)

You manage a Cisco VSG by placing it in service. You place the Cisco VSG in service by creating a compute firewall in an organization and assigning the Cisco VSG to that compute firewall.

You manage VMs by discovering those VMs which have a vNic listed in the port profile.

Resource Manager

Resource Manager manages Cisco VSGs, Nexus 1000V VSMs, and Virtual Center (VC). It also manages faults and events.

The Resource Manager provides the following management services:

- Allows the binding of organizations to resource pools.
- Integrates with VCs to retrieve VM attributes.
- Distributes VM attributes to Cisco VSGs.

- Retrieves VM IP addresses from Nexus 1000V VSM.
- Distributes VM IP addresses to Cisco VSGs.

Virtual Machines

Virtualization allows you to create multiple VMs that run in isolation, side by side on the same physical machine. Each VM has virtual RAM, a virtual CPU and NIC, and an operating system and applications. Because of virtualization, the operating system sees a consistent set of hardware regardless of the actual physical hardware components.

VMs are encapsulated in files for rapid saving, copying, and provisioning, which means that you can move full systems, configured applications, operating systems, BIOS, and virtual hardware within seconds, from one physical server to another. Encapsulated files allow for zero-downtime maintenance and continuous workload consolidation.

Instances of Cisco VNMC are installed on VMs.

Virtual Security Gateways

Cisco VSGs evaluate Cisco VNMC policies based on network traffic. The main functions of a Cisco VSG are as follows:

- Receives traffic from Virtual Network Service Data Path (vPath).

  For every new flow, the vPath component encapsulates the first packet and sends it to Cisco VSG as specified in the Nexus 1000V port profiles. It assumes that the Cisco VSG is Layer 2 adjacent to vPath. The mechanism used for communication between vPath and the Cisco VSG is similar to VEM and Nexus 1000V VSM communication on a packet VLAN.
- Performs application fix-up processing such as FTP, TFTP, and RSH.
- Evaluates policies by inspecting the packets sent by vPath using network, VM, and custom attributes.
- Transmits the policy evaluation results to vPath.

Each vPath component maintains a flow table for caching Cisco VSG policy evaluation results.

Virtual Security Gateways

Configuring a Compute Firewall

Adding a Compute Firewall

Important We recommend that you add the compute firewall object directly at the tenant level.

Procedure

Step 1 In the **Navigation** pane, click the **Resource Management** tab.

Step 2 In the **Navigation** pane, click the **Managed Resources** subtab.

Step 3 In the **Navigation** pane, expand the **root** > **Compute Firewalls** at the node you want to add a Compute Firewall.

Step 4 In the **Navigation** pane, click the **Compute Firewalls** node.

Step 5 In the **Work** pane, click the **Add Compute Firewall** link.

Step 6 In the **Add Compute Firewall** dialog box complete the following fields as appropriate:

Name	Description
Name field	The name of the object. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.
Description field	A user-defined description of the object.
Config State field	The configured state of the object. This field cannot be edited.

Table 29: Firewall Settings Area

Name	Description
Device Profile field	Click the **Select** button to open the **Select Firewall Device Profile** dialog box .
Management Hostname field	The management host name.
Data IP Address field	The data IP address. The vPath component running on each VEM uses the data IP address to determine the MAC address of the VSG (via ARP). Once the VSG MAC address has been resolved, vPath can communicate with the VSG using MAC in MAC encapsulation. Subsequently for each new flow initiated by a VM, vPath sends the first packet of the flow to the VSG for policy evaluation. vPath caches the VSG policy decision in a flow table. This is the same IP address which is configured in the **vn-service** CLI command on the Cisco Nexus 1000v port profile.
Data IP Subnet field	The data IP subnet.

Step 7 Click **OK**.

Editing a Compute Firewall

Procedure

Step 1 In the **Navigation** pane, click the **Resource Management** tab.
Step 2 In the **Navigation** pane, click the **Managed Resources** subtab.
Step 3 In the **Navigation** pane, expand the **root** > **Compute Firewalls** at the node you want to edit a compute firewall.
Step 4 In the **Navigation** pane, click the **Compute Firewalls** node.
Step 5 In the **Work** pane, click the compute firewall you want to edit.
Step 6 In the **Edit** dialog box, modify the following fields as appropriate:
a) On the **General** tab, change the description.
b) Modify the following as appropriate:

Table 30: Firewall Settings Area

Name	Description
Device Profile field	Click the **Select** link to open the **Select Firewall Device Profile** dialog box.
Management Hostname field	The management host name.
Data IP Address field	The data IP address. The vPath component running on each VEM uses the data IP address to determine the MAC address of the VSG (via ARP). Once the VSG MAC address has been resolved, vPath can communicate with the VSG using MAC in MAC encapsulation. Subsequently for each new flow initiated by a VM, vPath sends the first packet of the flow to the VSG for policy evaluation. vPath caches the VSG policy decision in a flow table. This is the same IP address which is configured in the **vn-service** CLI command on the Nexus 1000v port profile.
Data IP Subnet field	The data IP subnet.

Step 7 Click **OK**.

Deleting a Compute Firewall

Procedure

Step 1 In the **Navigation** pane, click the **Resource Management** tab.
Step 2 In the **Navigation** pane, click the **Managed Resources** subtab.
Step 3 In the **Navigation** pane, expand the **root** > **Compute Firewalls** at the node you want to delete a compute firewall.
Step 4 In the **Navigation** pane, click the **Compute Firewalls** node.
Step 5 In the **Work** pane, select the compute firewall you want to delete.
Step 6 Click the **Delete** link.
Step 7 In the **Confirm** dialog box, click **OK**.

Configuring a Pool

Adding a Pool

Procedure

Step 1 In the **Navigation** pane, click the **Resource Management** tab.
Step 2 In the **Navigation** pane, click the **Managed Resources** subtab.
Step 3 In the **Navigation** pane, expand the **root** > **Pools** node at the location where you want to add a pool.
Step 4 In the **Navigation** pane, click the **Pools** node.
Step 5 In the **Work** pane, click the **Add Pool** link.
Step 6 In the **Add Pool** dialog box, complete the following fields:

Table 31: Action Area

Name	Description
Name field	The name of the pool. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.

Name	Description
Description field	A description of the pool. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon. You cannot change this description after it is saved.

Step 7 (Optional) Assign pool members to the pool by performing the following tasks:

a) Click the **(Un)Assign** link.

b) In the **Assign Pool Member** dialog box, move the VSG you want to assign to the **Assigned VSGs** list..

c) Click **OK**.

Step 8 Click **OK**.

Editing a Pool

Procedure

Step 1 In the **Navigation** pane, click the **Resource Management** tab.

Step 2 In the **Navigation** pane, click the **Managed Resources** subtab.

Step 3 In the **Navigation** pane, expand **root** > **Pools** to where you want to edit a pool.

Step 4 In the **Navigation** pane, click the **Pools** node to view the **Pools** work pane.

Step 5 In the **Work** pane, click the pool you want to edit.

Step 6 In the **Edit** dialog box, modify as appropriate:

Name	Description
Name field	The name of the resource. You cannot edit this field.
Description field	A description of the resource. This name can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.

Table 32: Pool Members Area

Name	Description
(Un)Assign link	Click to open the **(Un)Assign Pool Members** dialog box. Use the dialog box to assign and unassign pool members.
IP Address column	A list of the IP addresses of the resources.
Compute Firewall column	A list of the compute firewalls.
Association State column	A list of the states of association of the resources.
Service ID column	A list of the service identification numbers for the resources.
Operational State column	A list of the operational states of the resources.

Note Depending upon the object you select in the table, different options will appear in the area above the table.

Step 7 Click **OK**.

Deleting a Pool

Procedure

Step 1 In the **Navigation** pane, click the **Resource Management** tab.
Step 2 In the **Navigation** pane, click the **Managed Resources** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Pools** to where you want to delete a pool.
Step 4 In the **Navigation** pane, click the **Pools** node to view the **Pools** work pane.
Step 5 In the **Work** pane, click the pool you want to delete.
Step 6 Click the **Delete** link.
Step 7 In the **Confirm** dialog box, click **OK**.

Assigning and Unassigning VSGs and Pools

Assigning a VSG

Procedure

Step 1 In the **Navigation** pane, click the **Resource Management** tab.
Step 2 In the **Navigation** pane, click the **Managed Resources** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Compute Firewalls** to the node where you want to assign a VSG.
Step 4 In the **Navigation** pane, click the compute firewall where you want to assign a VSG.
Step 5 In the **Work** pane, click the **Assign VSG** link.
Step 6 In the **Assign VSG** dialog box, select the desired IP address from the **VSG Management IP** drop-down list.
Step 7 Click **OK**.

Assigning a Pool

Procedure

Step 1 In the **Navigation** pane, click the **Resource Management** tab.
Step 2 In the **Navigation** pane, click the **Managed Resources** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Compute Firewalls** to the node where you want to assign a pool
Step 4 In the **Navigation** pane, click the compute firewall where you want to assign a pool.
Step 5 In the **Work** pane, click the **Assign Pool** link.
Step 6 In the **Assign Pool** dialog box, select the desired pool from the **Name** drop-down list.
Step 7 Click **OK**.

Unassigning a VSG and Pool

Procedure

Step 1 In the **Navigation** pane, click the **Resource Management** tab.
Step 2 In the **Navigation** pane, click the **Managed Resources** subtab.
Step 3 In the **Navigation** pane, expand the **root** node.
Step 4 Click the *Compute Firewall_name* where you want to unassign a VSG and pool.
Step 5 In the **Work** pane, click the **Unassign VSG/Pool** link.
Step 6 In the **Confirm** dialog box, click **Yes**.

CHAPTER 12

Configuring Backups

This chapter includes the following sections:

Restoring the Cisco VNMC Software to the Backup Configuration

Restoring the Cisco VNMC Software to the Backup Configuration

Procedure

Step 1 Install the Cisco VNMC virtual machine (VM).
For details, see the *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(3) and Cisco Virtual Network Management Center, Release 1.3 Installation and Upgrade Guide*.

Step 2 Uninstall the Cisco VSG policy agents.
Connect the Secure Shell to the Cisco VSG console for this task. This step does not cause a traffic disruption.

Example:
```
vsg# conf t
vsg (config)# vnm-policy-agent
vsg (config-vnm-policy-agent)# no policy-agent-image
```
Note Perform this step for all Cisco VSGs that are associated with the Cisco VNMC that you are restoring.

Step 3 Uninstall the VSM policy agents.
Connect the Secure Shell to the VSM console for this task. This step does not cause a traffic disruption.

Example:
```
vsm# conf t
vsm (config)# vnm-policy-agent
vsm (config-vnm-policy-agent)# no policy-agent-image
```
Note Perform this step for all VSMs that are associated with the Cisco VNMC you are restoring.

Step 4 Restore the Cisco VNMC database.
Connect the Secure Shell to the Cisco VNMC CLI for this task. Depending upon your Cisco VNMC backup location, restore using File Transfer Protocol (FTP), Secure Copy (SCP), Trivial File Transfer Protocol (TFTP), or Secure File Transfer Protocol (SFTP).

Example:
```
vnmc# connect local-mgmt
vnmc(local-mgmt)# restore scp://[username@]server[/path]
```
Step 5 In the Cisco VNMC GUI, click **Administration** > **Service Registry** > **Clients**, and in the **Work** pane do the following:

a) Wait until each registered VSM displays the operational status as lost-visibility.

b) Choose each VSM, and click the **Delete Client** icon.

Step 6 In the Cisco VNMC GUI, click **Resource Management** > **Resources** > **Virtual Supervisor Modules**, and verify that the deleted VSMs are not visible.

Step 7 Reinstall the VSM policy agents.
Note If the VSM policy agents must be upgraded, install the new software now.

Example:
```
VSM# conf t
VSM (config)# vnm-policy-agent
VSM (config-vnm-policy-agent)# policy-agent-image bootflash:vnmc-vsmpa.1.0.1g.bin
```
Step 8 Wait until all the VSMs have registered in the Service Registry and are displayed under **Resource Management** > **Resources** > **Virtual Supervisor Modules**.

Step 9 Reinstall the Cisco VSG policy agents.
Note If the Cisco VSG policy agents must be upgraded, install the new software now.

Example:
```
VSG# conf t
VSG (config)# vnm-policy-agent
VSG (config-vnm-policy-agent)# policy-agent-image bootflash:vnmc-vsgpa.1.0.1g.bin
```
Step 10 Verify the following states after the restore process is complete:
Note The restore process could take a few minutes depending upon your setup environment.

a) On the Cisco VSG CLI, verify that your configurations are restored to their earlier state.

b) On the Cisco VNMC GUI, verify that your objects and policies are restored to their earlier state.

Configuring Backup Operations

Creating a Backup Operation

Before You Begin

Obtain the backup server IP address and authentication credentials.

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.

Step 2 In the **Navigation** pane, click the **Operations** subtab.

Step 3 In the **Navigation** pane, click the **Backups** node.

Step 4 In the **Work** pane, click the **Create Backup Operation** link.

Step 5 In the **Create Backup Operation** dialog box, complete the following fields:

Name	Description
Admin State radio button	The administrative state. This can be one of the following states: • **enabled**—Backup is enabled. The system runs the backup operation as soon as you click **OK**. • **disabled**—Backup is disabled. The system does not run the backup operation when you click **OK**. If you select this option, all fields in the dialog box remain visible.
Type field	The type of backup. It creates a copy of the whole database file. You can use this file for disaster recovery if you need to recreate every configuration on your. This field is not editable.
Protocol radio button	The protocol used when communicating with the remote server. This can be one of the following protocols: • **ftp** • **scp** • **sftp** • **tftp**

Name	Description
Hostname field	The hostname or IP address of the device the backup file is stored. The hostname cannot be changed when editing the operation. **Note** If you use a hostname rather than an IP address, you must configure a DNS server.
User field	The user name the system uses to log into a remote server. This field is not displayed if the protocol chosen is tftp.
Password field	The password the system uses to log into a remote server. This field does not appear if the protocol chosen is TFTP. **Note** Cisco VNMC does not store this password. You do not need to enter this password unless you intend to enable and run the backup operation immediately.
Absolute Path Remote File field	The full path to the backup configuration file. This field can contain the filename as well as the path. If you omit the filename, the backup procedure assigns a name.

Step 6 Click **OK**.

Running a Backup Operation

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **Operations** subtab.
Step 3 In the **Navigation** pane, click and expand the **Backups** node.
Step 4 In the **Navigation** pane, click the file you want to run.
Step 5 In the **Work** pane, click the **General** tab.
Step 6 In the **Properties** area, complete the following fields:
a) In the **Admin State** field, click the **enabled** button.

b) For all the protocols, except TFTP, enter the password for the username in the **Password** field.
c) (Optional) Change the content of the other available fields.

Step 7 Click **Save**.
Cisco VNMC takes a snapshot of the configuration type that you selected and exports the file to the network location.

Step 8 (Optional) To view the progress of the backup operation, click the **Task** tab in the pane. The backup operation continues to run until it is completed.

Editing a Backup Operation

Before You Begin

Obtain the backup server IP address and authentication credentials.

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **Operations** subtab.
Step 3 In the **Navigation** pane, click the **Backups** node.
Step 4 In the **Work** pane, expand the items in the table, and select the backup operation you want to edit.
Step 5 In the **Edit** dialog box, modify the following fields as appropriate:

Name	Description
Admin State radio button	The administrative state. This can be one of the following states: • **enabled**—Backup is enabled. The system runs the backup operation as soon as you click **OK**. • **disabled**—Backup is disabled. The system does not run the backup operation when you click **OK**. If you select this option, all fields in the dialog box remain visible.
Type field	The type of backup. It creates a copy of the whole database file. You can use this file for disaster recovery if you need to recreate every configuration on your. This field is not editable.

Name	Description
Protocol radio button	The protocol used when communicating with the remote server. This can be one of the following protocols: • **ftp** • **scp** • **sftp** • **tftp**
Hostname field	The hostname or IP address of the device the backup file is stored. The hostname cannot be changed when editing the operation. **Note** If you use a hostname rather than an IP address, you must configure a DNS server.
User field	The user name the system uses to log into a remote server. This field is not displayed if the protocol chosen is tftp.
Password field	The password the system uses to log into a remote server. This field does not appear if the protocol chosen is TFTP. **Note** Cisco VNMC does not store this password. You do not need to enter this password unless you intend to enable and run the backup operation immediately.
Absolute Path Remote File field	The full path to the backup configuration file. This field can contain the filename as well as the path. If you omit the filename, the backup procedure assigns a name.

Step 6 Click **OK**.

Deleting a Backup Operation

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **Operations** subtab.
Step 3 In the **Navigation** pane, click **Backups** node.
Step 4 In the **Work** pane, click the backup operation you want to delete.
Step 5 Click the **Delete** link.
Step 6 In the **Confirm** dialog box, click **OK**.

Configuring Import Operations

Creating an Import Operation

Before You Begin

Obtain the backup server IP address and authentication credentials.

Important The association of compute firewalls with VSGs are not included in the export or import data. Only the compute firewall definitions are included, such as device profiles and policies. Therefore, if an imported compute firewall did not exist in the system, it will not be associated to any VSG after the import operation. If an imported firewall already existed in the system, the association state remains the same.

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **Operations** subtab.
Step 3 In the **Navigation** pane, click the **Backups** node.
Step 4 In the **Work** pane, click the **Create Import Operation** link.
Step 5 In the **Create Import Operation** dialog box, complete the following fields:

Name	Description
Admin State radio button	The administrative state. This can be one of the following states: • **enabled**—Import is enabled. The system runs the backup operation as soon as you click **OK**. • **disabled**—Import is disabled. The system does not run the backup operation when you click **OK**. If you select this option, all fields in the dialog box remain visible.
Action radio button	The action to be taken on a file. Currently, the only action is **merge**.
Protocol radio button	The protocol used when communicating with the remote server. This can be one of the following protocols: • **ftp** • **scp** • **sftp** • **tftp**
Hostname field	The hostname or IP address of the device the backup file is stored. The hostname cannot be changed when editing the operation. **Note** If you use a hostname rather than an IP address, you must configure a DNS server.
User field	The user name the system uses to log into a remote server. This field does not apply if the protocol is tftp.
Password field	The password the system uses to log into a remote server. This field does not appear if the protocol chosen is TFTP. **Note** Cisco VNMC does not store this password. You do not need to enter this password unless you intend to enable and run the backup operation immediately.
Absolute Path Remote File(.tgz) field	The absolute path to the .tgz file.

Step 6 Click **OK**.

Editing an Import Operation

Before You Begin

Obtain the backup server IP address and authentication credentials.

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.

Step 2 In the **Navigation** pane, click the **Operations** subtab.

Step 3 In the **Navigation** pane, click the **Backups** node.

Step 4 In the **Work** pane, expand the items in the table, and select the import operation you want to edit.

Step 5 Click the **Edit** link.

Step 6 In the **Edit** dialog box, modify the fields as appropriate:

Name	Description
Admin State radio button	The administrative state. This can be one of the following states: • **enabled**—Import is enabled. The system runs the backup operation as soon as you click **OK**. • **disabled**—Import is disabled. The system does not run the backup operation when you click **OK**. If you select this option, all fields in the dialog box remain visible.
Action radio button	The action to be taken on a file. Currently, the only action is **merge**.
Protocol radio button	The protocol used when communicating with the remote server. This can be one of the following protocols: • **ftp** • **scp** • **sftp** • **tftp**

Name	Description
Hostname field	The hostname or IP address of the device the backup file is stored. The hostname cannot be changed when editing the operation. **Note** If you use a hostname rather than an IP address, you must configure a DNS server.
User field	The user name the system uses to log into a remote server. This field does not apply if the protocol is tftp.
Password field	The password the system uses to log into a remote server. This field does not appear if the protocol chosen is TFTP. **Note** Cisco VNMC does not store this password. You do not need to enter this password unless you intend to enable and run the backup operation immediately.
Absolute Path Remote File(.tgz) field	The absolute path to the .tgz file.

Step 7 Click **OK**.

Deleting an Import Operation

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **Operations** subtab.
Step 3 In the **Navigation** pane, click the **Backups** node.
Step 4 In the **Work** pane, click the import operation you want to delete.
Step 5 Click the **Delete** link.
Step 6 In the **Confirm** dialog box, click **Yes**.

Configuring Export Operations

Creating an Export Operation

Before You Begin

Obtain the backup server IP address and authentication credentials before performing an export.

Important The associations of compute firewalls with VSGs are not included in export or import data. Only compute firewall definitions are included, such as device profiles and policies. If an imported compute firewall did not exist in the system, it will not be associated to any VSG after the import operation. If an imported firewall already existed in the system, the association state remains the same.

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.

Step 2 In the **Navigation** pane, click the **Operations** subtab.

Step 3 In the **Navigation** pane, click the **Backups** node.

Step 4 In the **Work** pane, click the **Create Export Operation** link.

Step 5 In the **Create Export Operation** dialog box, complete the following fields:

Name	Description
Admin State radio button	The administrative state. This can be one of the following states: • **enabled**—Export is enabled. The system runs the backup operation as soon as you click **OK**. • **disabled**—Export is disabled. The system does not run the backup operation when you click **OK**. If you select this option, all fields in the dialog box remain visible.
Type radio button	The type of backup. This can be one of the following types: • **config-all** • **config-logical** • **config-system**

Name	Description
Protocol radio button	The protocol used when communicating with the remote server. This can be one of the following protocols: • **ftp** • **scp** • **sftp** • **tftp**
Hostname field	The hostname or IP address of the device the backup file is stored. The hostname cannot be changed when editing the operation. **Note** If you use a hostname rather than an IP address, you must configure a DNS server.
User field	The user name the system uses to log into a remote server. This field is not displayed if the protocol is tftp.
Password field	The password the system uses to log into a remote server. This field does not appear if the protocol chosen is TFTP. **Note** Cisco VNMC does not store this password. You do not need to enter this password unless you intend to enable and run the backup operation immediately.
Absolute Path Remote File(.tgz) field	The absolute path to the .tgz file.

Step 6 Click **OK**.

Editing an Export Operation

Before You Begin

Obtain the backup server IP address and authentication credentials.

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.

Step 2 In the **Navigation** pane, click the **Operations** subtab.

Step 3 In the **Navigation** pane, click the **Backups** node.

Step 4 In the **Work** pane, expand the items in the table, and select the export operation you want to edit.

Step 5 Click the **Edit** link.

Step 6 In the **Edit** dialog box, modify the fields as appropriate:

Name	Description
Admin State radio button	The administrative state. This can be one of the following states: • **enabled**—Export is enabled. The system runs the backup operation as soon as you click **OK**. • **disabled**—Export is disabled. The system does not run the backup operation when you click **OK**. If you select this option, all fields in the dialog box remain visible.
Type radio button	The type of backup. This can be one of the following types: • **config-all** • **config-logical** • **config-system**
Protocol radio button	The protocol used when communicating with the remote server. This can be one of the following protocols: • **ftp** • **scp** • **sftp** • **tftp**
Hostname field	The hostname or IP address of the device the backup file is stored. The hostname cannot be changed when editing the operation. **Note** If you use a hostname rather than an IP address, you must configure a DNS server.

Name	Description
User field	The user name the system uses to log into a remote server. This field is not displayed if the protocol is tftp.
Password field	The password the system uses to log into a remote server. This field does not appear if the protocol chosen is TFTP. **Note** Cisco VNMC does not store this password. You do not need to enter this password unless you intend to enable and run the backup operation immediately.
Absolute Path Remote File(.tgz) field	The absolute path to the .tgz file.

Step 7 Click **OK**.

Deleting an Export Operation

Procedure

Step 1 In the **Navigation** pane, click the **Administration** tab.
Step 2 In the **Navigation** pane, click the **Operations** subtab.
Step 3 In the **Navigation** pane, click the **Backups** node.
Step 4 In the **Work** pane, click the export operation you want to delete.
Step 5 Click the **Delete** link.
Step 6 In the **Confirm** dialog box, click **Yes**.

INDEX

E

F

L

M

N

O

P

R

S

T

U

V

W