Cisco Prime Network Services Controller 3.4.2b User Guide

First Published: 2017-03-31

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **Overview** 1

Prime Network Services Controller Overview 1

Topology Examples 2

Features and Benefits 2

CHAPTER 2 **Getting Started** 5

Logging Into 5

Configuration Workflow 5

GUI Overview 6

User Interface Components 6

Toolbar 7

Tables 8

Field Aids 8

Firewall Access 9

Setting the Idle Timeout Period - Preferences 10

Search 10

Clone 11

CHAPTER 3 **Configuring RBAC** 13

RBAC 13

User Accounts 13

Username Guidelines 14

Password Guidelines 14

User Roles 15

Privileges 17

User Locales 18

Configuring User Roles 19

Creating a User Role 19

Editing a User Role 20
Deleting a User Role 20
Configuring User Locales 21
Creating a Locale 21
Editing a Locale 22
Deleting a Locale 22
Assigning an Organization to a Locale 23
Deleting an Organization from a Locale 23
Configuring Locally Authenticated User Accounts 24
Creating a User Account 24
Changing the Locales or Roles Assigned to a Locally Authenticated User 28
Monitoring User Sessions 28

CHAPTER 4 Configuring Primary Authentication 31
Primary Authentication 31
Remote Authentication Providers 31
Creating an LDAP Provider 32
Editing an LDAP Provider 34
Deleting an LDAP Provider 35
Selecting a Primary Authentication Service 35

CHAPTER 5 Configuring Trusted Points 37
Trusted Points 37
Configuring Trusted Points 37
Creating a Trusted Point 37
Editing a Trusted Point 38
Deleting a Trusted Point 38

CHAPTER 6 Configuring VM Managers 39
VM Manager Overview 39
Hypervisor and VMM Support 40
Configuring Connectivity with VMware vCenter 41
Exporting the vCenter Extension File 41
Registering the vCenter Extension Plugin in vCenter 42
Configuring Connectivity with vCenter 43

Configuring Connectivity with Microsoft SCVMM 44
Editing a VM Manager 45
Deleting a VM Manager 47

CHAPTER 7 Configuring System Profiles 49
System Profile Overview 49
Policies in Profiles 49
Configuring Policies 50
Configuring a Core File Policy Profile 50
Core File Attributes Table 51
Configuring a Fault Policy 51
Fault Policy Attributes Table 52
Configuring a Logging Policy 53
Logging Policy Attributes Tables 53
Configuring a Syslog Policy 54
Syslog Policy Attributes Table 55
Adding a Syslog Server to a Syslog Policy 57
Syslog Server Attributes Table 58
Modifying the Default Profile 60
Editing a DNS Domain 62
Adding an NTP Server 62

CHAPTER 8 Configuring Tenants 65
Tenant Management 65
Tenant Management and Multi-Tenant Environments 65
Name Resolution in a Multi-Tenant Environment 66
Configuring Tenants 67
Creating a Tenant 67
Editing a Tenant 67
Deleting a Tenant 68
Configuring Virtual Data Centers 68
Creating a Virtual Data Center 68
Editing a Virtual Data Center 69
Deleting a Virtual Data Center 69
Configuring Applications 70

Creating an Application 70
Editing an Application 70
Deleting an Application 71
Configuring Tiers 71
Creating a Tier 71
Editing a Tier 72
Deleting a Tier 72

CHAPTER 9 Configuring Service Policies and Profiles 75
Service Path Configuration Workflow 75
Prerequisites for Configuring Service Paths 76
Adding a Port Profile to a VSM 77
Creating a Service Node 78
Creating a Service Path 79
Binding a Service Path to a Port Profile 80
Configuring Service Policies 81
Configuring ACL Policies and Policy Sets 82
Adding an ACL Policy 82
Add ACL Policy Rule Dialog Box 83
Time Ranges in ACL Policy Rules 86
Adding an ACL Policy Set 87
Configuring Connection Timeout Policies 88
Add Connection Timeout Policy Rule Dialog Box 89
Configuring DHCP Policies 90
Adding a DHCP Relay Server 90
Add DHCP Relay Server Dialog Box 91
Configuring a DHCP Relay Policy 91
Add DHCP Relay Policy Dialog Box 91
Configuring a DHCP Server Policy 92
Add DHCP Server Policy Dialog Box 92
Configuring IP Audit and IP Audit Signature Policies 93
Configuring IP Audit Policies 94
Add IP Audit Policy Rule Dialog Box 94
Configuring IP Audit Signature Policies 95
Configuring NAT/PAT Policies and Policy Sets 96

Configuring NAT/PAT Policies 96
Add NAT Policy Rule Dialog Box 97
Configuring NAT Policy Sets 98
Configuring PAT for Edge Firewalls 99
Configuring Source Dynamic Interface PAT 99
Configuring Destination Static Interface PAT 100
Configuring Packet Inspection Policies 101
Protocols Supported for Packet Inspection Policies 102
Add Packet Inspection Policy Rule Dialog Box 102
Configuring Routing Policies 103
Configuring TCP Intercept Policies 103
Add TCP Intercept Policy Rule Dialog Box 104
Configuring Site-to-Site IPsec VPN Policies 105
Configuring Crypto Map Policies 105
Add Crypto Map Policy Dialog Box 106
Add Crypto Map Policy Rule Dialog Box 107
Configuring IKE Policies 108
IKE V1 Policy Dialog Box 110
IKE V2 Policy Dialog Box 110
Configuring Interface Policy Sets 110
Add Interface Policy Set Dialog Box 111
Configuring IPsec Policies 112
IPsec IKEv1 Proposal Dialog Box 113
IPsec IKEv2 Proposal Dialog Box 114
Configuring Peer Authentication Policies 114
Add Policy to Authenticate Peer Dialog Box 115
Configuring VPN Device Policies 116
Add VPN Device Policy Dialog Box 117
Configuring Zone-Based Firewall Policies 119
Working with Profiles 120
Configuring Compute Security Profiles 120
Add Compute Security Profile Dialog Box 121
Verifying Compute Firewall Policies 122
Configuring Edge Device Profiles 122
Edge Device Profile Dialog Box 123

Configuring Edge Security Profiles 124
Add Edge Security Profile Dialog Box 125
Applying an Edge Device Profile 126
Applying an Edge Security Profile 126
Verifying Edge Firewall Policies 127
Configuring Security Profiles 128
Editing a Security Profile for a Compute Firewall 128
Editing a Security Profile for an Edge Firewall 129
Deleting a Security Profile 131
Deleting a Security Profile Attribute 132
Assigning a Policy 132
Unassigning a Policy 133
Configuring Security Policy Attributes 133
Configuring Object Groups 133
Adding an Object Group 133
Adding an Object Group Expression 134
Editing an Object Group 135
Editing an Object Group Expression 136
Deleting an Object Group 137
Deleting an Object Group Expression 137
Configuring Security Profile Dictionary 138
Adding a Security Profile Dictionary 138
Adding a Security Profile Dictionary Attribute 139
Editing a Security Profile Dictionary 139
Editing a Security Profile Dictionary Attribute 140
Deleting a Security Profile Dictionary 141
Deleting a Security Profile Dictionary Attribute 141
Working with vZones 141
Adding a vZone 142
Editing a vZone 143
Deleting a vZone Condition 144
Deleting a vZone 145

CHAPTER 10 **Configuring Device Policies and Profiles** 147
Device Policies and Profiles 147

Device Profiles 147
Policies 148
Device Configuration 148
Device Policies 149
Configuring Device Policies 149
Configuring AAA Policies 149
Field Descriptions 151
Add Authentication Policy Dialog Box 151
Remote Access Method Dialog Box 152
Login Authentication Method Dialog Box 153
Configuring Authorization Policies 153
Add Authorization Policy Dialog Box 154
Authorization Method Dialog Box 155
Configuring Accounting Policy 155
Add Accounting Policy Dialog Box 156
Configuring Global Server Timers 156
Add Global Server Timers Dialog Box 157
Configuring Core File Policies 157
Adding a Core File Policy for a Device 157
Editing a Core File Policy for a Device Profile 158
Deleting a Core File Policy from a Device Profile 159
Configuring Fault Policies 160
Adding a Fault Policy for a Device Profile 160
Editing a Fault Policy for a Device Profile 161
Deleting a Fault Policy for a Device Profile 162
Configuring Log File Policies 163
Adding a Logging Policy for a Device Profile 163
Editing a Logging Policy for a Device Profile 164
Deleting a Logging Policy for a Device Profile 166
Configuring SNMP Policies 166
Adding an SNMP Policy 166
Editing an SNMP Policy 168
Deleting an SNMP Policy 170
Adding an SNMP Trap Receiver 171
Editing an SNMP Trap Receiver 172

Deleting an SNMP Trap Receiver 172
Configuring Syslog Policies 173
Adding a Syslog Policy for a Device 173
Field Descriptions 173
Add Syslog Policy Dialog Box 173
Editing a Syslog Policy for a Device Profile 176
Deleting a Syslog Policy for a Device Profile 178
Adding a Syslog Server for a Device Profile 179
Field Descriptions 180
Add Syslog Server Dialog Box 180
Editing a Syslog Server for a Device Profile 182
Deleting a Syslog Server for a Device Profile 184
Configuring Device Profiles 185
Adding a Firewall Device Profile 185
Editing a Firewall Device Profile 186
Deleting a Firewall Device Profile 189
Configuring NTP 189
Creating a Device Profile with NTP 190
Field Descriptions 191
Add NTP Server Dialog Box 191
Applying Device Profiles to Compute Firewalls 191
Applying Device Profiles to Edge Firewalls 192
Associating Device Policies with Profiles 192

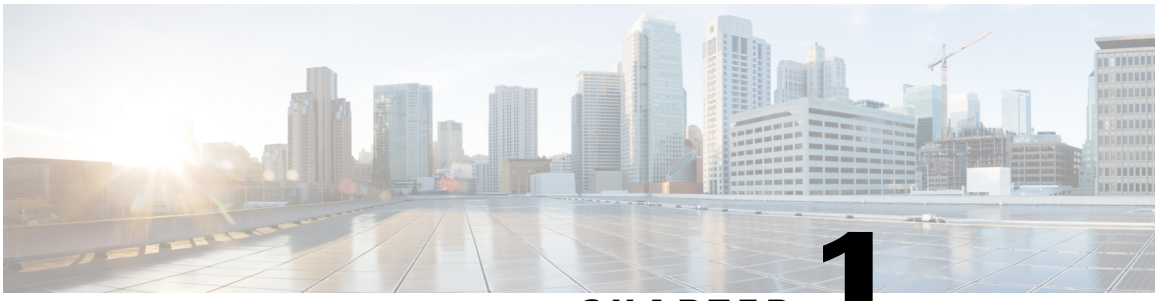
CHAPTER 11 **Configuring Managed Resources** 195
Resource Management 195
Resource Management Configuration Workflow 196
Registering Third-Party VMs in VMware 196
Deploying the Prime Network Services Controller Device Adapter on VMware 197
Deploying a Citrix NetScaler Load Balancer on VMware 198
Verifying VM Registration 200
Importing Service Images 200
Compute Firewalls 201
Adding a Compute Firewall 201
Compute Firewall Deployment Options 203

Field Descriptions 203
Properties Screen 203
Service Device Screen 204
Managing Compute Firewalls 204
Unassigning a VSG 207
Edge Firewalls 207
Adding an Edge Firewall 207
Field Descriptions 210
Properties Screen 210
Unassigning an ASA 1000V 210
Edge Routers 211
Edge Router Configuration Workflow 211
Prerequisites for Configuring Edge Routers 212
Adding Edge Routers 213
Edge Router Deployment Options 214
Managing Edge Routers 215
Load Balancers 216
Load Balancer Configuration Workflow 216
Prerequisites for Configuring Load Balancers 216
Adding Load Balancers 218
Load Balancing Service Dialog Boxes 219
Security Policy Dialog Boxes 220
Managing Load Balancers 221
Adding a Port Profile to a VSM 222
Updating Discovered VSM Port Profiles 223
Troubleshooting Devices and Services 224
Launching ASDM 224
Managing VSG Pools 226
Adding a VSG Pool 226
Assigning a VSG Pool 227
Editing a VSG Pool 227
Unassigning a VSG Pool 227
Deleting a VSG Pool 228

CHAPTER 12 **Integrating with DCNM** 229

DCNM Integration Overview 229
Configuring Connectivity with DCNM 232
Troubleshooting Integration Issues 233

CHAPTER 13 **Configuring Administrative Operations 237**
Administrative Operation Conventions 237
Managing Backup Operations 237
Creating a Backup Operation 238
Running a Backup Operation 239
Editing a Backup Operation 240
Deleting a Backup Operation 242
Restoring a Backup Configuration 242
Managing Export Operations 246
Creating an Export Operation 247
Editing an Export Operation 248
Deleting an Export Operation 250
Configuring Import Operations 250
Creating an Import Operation 250
Editing an Import Operation 252
Deleting an Import Operation 253



CHAPTER 1

Overview

This section contains the following topics:

- Prime Network Services Controller Overview, page 1
- Topology Examples, page 2
- Features and Benefits, page 2

Prime Network Services Controller Overview

The dynamic nature of cloud environments requires organizations to apply and enforce frequent changes to networks. These networks can consist of thousands of virtual services elements, such as firewalls, load balancers, routers, and switches. simplifies operations with centralized, automated multi-device and policy management for Cisco network virtual services. For the latest release updates and overview, see the corresponding data sheet.

() is the primary management element for Cisco Nexus 1000V (Nexus 1000V) Switches and Services that can enable a transparent, scalable, and automation-centric network management solution for virtualized data center and hybrid cloud environments. Nexus 1000V switches and services deliver a highly secure multitenant environment by adding virtualization intelligence to the data center network. These virtual switches are built to scale for cloud networks. Support for Virtual Extensible LAN (VXLAN) helps enable a highly scalable LAN segmentation and broader virtual machine (VM) mobility.

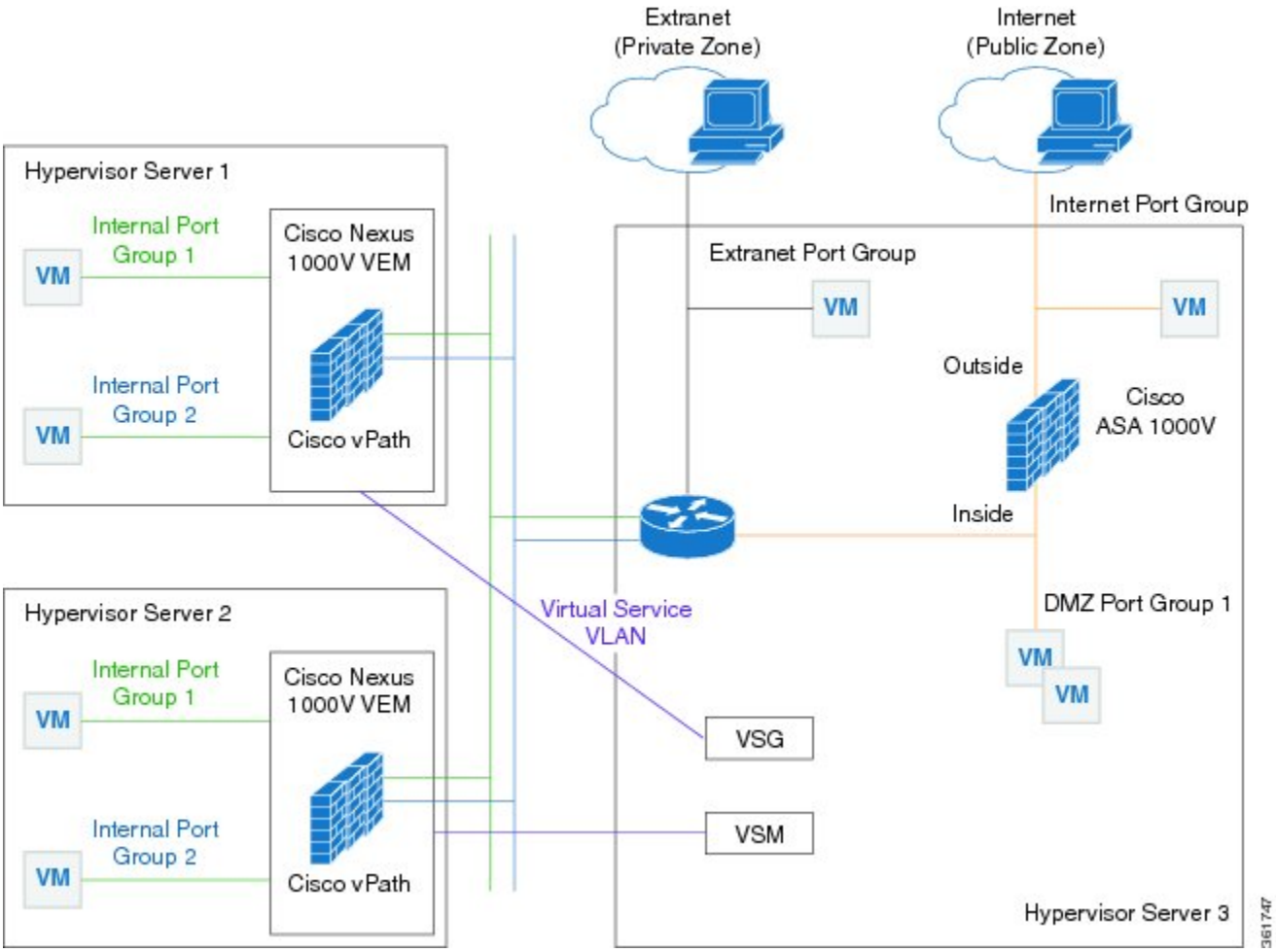
enables the centralized management of Cisco virtual services to be performed by an administrator, through its GUI, or programmatically through its XML API. is built on an information-model architecture in which each managed device is represented by its subcomponents (or objects), which are parametrically defined. This model-centric approach enables a flexible and simple mechanism for provisioning and securing virtualized infrastructure using Cisco VSG security services.

Note Starting with Cisco PNSC Release 3.4.2a, Cisco Adaptive Security Appliance (ASA 1000V), Cisco Cloud Services Router (CSR), Citrix NetScaler VPX, Citrix NetScaler, and KVM Hypervisor, and Microsoft HyperV platforms are not supported.

Topology Examples

The following figures show virtual data center examples.

Figure 1: Virtual Data Center Topology Example



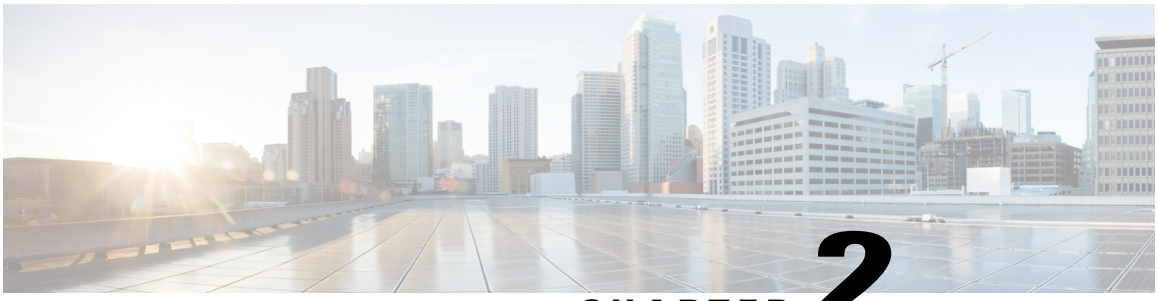
Features and Benefits

The following table lists the features and benefits of using .

Features	Description	Benefits
Multiple-Device Management	Prime Network Services Controller provides central management of installed VMs (edge routers, edge firewalls, compute firewalls, and load balancers) and Nexus 1000V. **Note** Citrix NetScaler VPX, CSR 1000V and ASA 1000V are supported in PNSC release 3.4.1d or earlier. Starting with Cisco PNSC release 3.4.2a, only Cisco VSG is supported.	Simplifies provisioning and troubleshooting in a scaled-out data center.
Security Profiles	A security profile represents the VSG security policy configuration in a profile (template).	Simplifies provisioning, reduces administrative errors during security policy changes, reduces audit complexities, and helps enable a highly scaled-out data center environment.
Stateless Device Provisioning	The management agents in VSG are stateless, receiving information from .	• Enhances scalability. • Provides robust endpoint failure recovery without loss of configuration state.
Security Policy Management	Security policies are authored, edited, and provisioned centrally.	• Simplifies operation and management of security policies. • Helps ensure that security intent is accurately represented in the associated security policies.
Context-Aware Security Policies	obtains virtual machine contexts from VMware vCenter.	Allows a security administrator to institute highly specific policy controls across the entire virtual infrastructure.
Support virtual services for DFA environments	Cisco Prime NSC obtains tenant information and allows virtual services to be added to DFA virtual overlay networks.	—

Features	Description	Benefits
Dynamic Security Policy and Zone Provisioning	interacts with the Nexus 1000V VSM to bind the security profile to the corresponding Nexus 1000V port profile. When virtual machines are dynamically instantiated by server administrators and appropriate port profiles applied, their association with trust zones is also established.	Helps enable security profiles to stay aligned with rapid changes in the virtual data center.
Multi-Tenant (Scale-Out) Management	is designed to manage VSG security policies in a dense multi-tenant environment so that administrators can rapidly add and delete tenants and update tenant-specific configurations and security policies.	Reduces administrative errors, helps ensure segregation of duties in administrative teams, and simplifies audit procedures.
Role-Based Access Control (RBAC)	RBAC simplifies operational tasks across different types of administrators, while allowing subject-matter experts to continue with their normal procedures.	• Reduces administrative errors. • Enables detailed control of user privileges. • Simplifies auditing requirements.
XML-Based API	XML API allows external system management and orchestration tools to programmatically provision VSG .	• Allows the use of the best-in-class management software. • Offers transparent and scalable operation management.

Note Citrix NetScaler VPX, CSR 1000V, and ASA 1000V are supported in PNSC release 3.4.1d or earlier. Hypervisors Openstack KVM and Microsoft HyperV are supported in PNSC releases up to 3.4.1d.



CHAPTER 2

Getting Started

This section contains the following topics:

- Logging Into , page 5
- Configuration Workflow, page 5
- GUI Overview, page 6

Logging Into

The default HTTPS URL for logging into the user interface is https://*server-ip-address*, where *server-ip-address* is the IP address assigned to the server. The IP address is the address for the management port.

Note If you log in using HTTP, you are automatically redirected to the HTTPS link.

Configuration Workflow

The following table provides the most common initial and ongoing workflow tasks to configure .

Initial Configuration Tasks (Administrative)	Description
1. User Roles	Configure roles for user access.
2. Primary Authentication	Configure LDAP providers and select a primary authentication service.
3. Creating a Trusted Point	Configure trusted points for LDAP over SSL.
4. Configuring VM Managers	Configure access with hypervisors.
5. Configuring Device Policies and Profiles	Configure the default system profile.

Initial Configuration Tasks (Administrative)	Description
Ongoing Configuration Tasks	
6. Creating a Tenant	Add tenants for resource and service support.
7. Configuring Service Policies and Profiles	Configure access and security-related policies for access to resources.
8. Configuring Device Policies and Profiles	Configure device-specific policies and profiles.
9. Configuring Managed Resources, on page 195	Add and configure enterprise and cloud resources. **Note** To instantiate a cloud VM, use Cisco Intercloud Fabric to import the cloud template before instantiation in Cisco Prime Network Services Controller.

GUI Overview

provides a browser-based interface that enables you to configure managed endpoints, perform administrative operational tasks, and define and apply policies and profiles. You also use the GUI to manage and provision device resources.

User Interface Components

When you log into , the user interface is displayed.

The user interface contains the components described in the following table:

Table 1: User Interface Components

Component	Description
Title	Displays "."
Toolbar	Allows you to set inactivity timeout values, obtain product version information, access online help, provide product feedback, and log out.
Tabs	Provide access to the primary components for managing your environment: • Tenant Management • Resource Management • Policy Management • Administration

Component	Description
Navigation pane	Provides navigation to all objects in the instance. The navigation pane is displayed on the left side of the screen below the tabs. The objects that are displayed in the navigation pane depend on the selected tab.
Content pane	Displays information and provides options for the object that is selected in the navigation pane. The Content pane often includes tables.

The following table provides information about the tabs in the GUI:

Table 2: Tabs in the GUI

Tab	Description
Tenant Management	Enables you to manage tenants in the current instance. A system or server administrator can use this tab to create organizational hierarchies and enable multi-tenant management domains. The organizational hierarchy levels are Tenant > Virtual Data Center > Application > Tier.
Resource Management	Enables you to manage logical resources, such as VSGs, ASA 1000Vs, VSGs, and vCenters.
Policy Management	Enables you to configure service and device policies and profiles, and to assign policies to profiles.
Administration	Provides the tools needed for administering .

Toolbar

The toolbar displays in the upper-right portion of the user interface. The following table describes the toolbar options:

Table 3: Toolbar Options

Option	Description
(*username*)	Username of the current session.
Preferences	Enables you to specify the amount of time that the session can remain inactive before the session times out. The value that you specify applies to the system from which you logged into .
Log Out	Logs you out of the current session.
About	Provides version information.

Option	Description
Help	Launches online help for the currently displayed screen.
Feedback	Allows you to provide feedback on .

Tables

The tables in the GUI contain the following features:

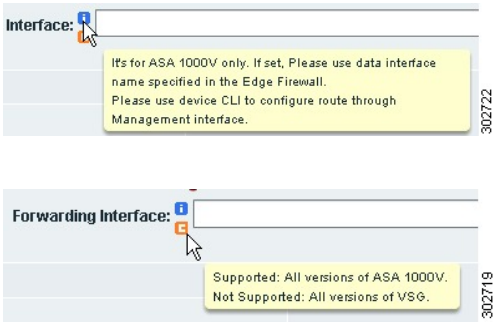
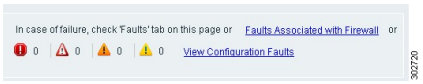
Feature	Description
Actions drop-down list	For tables that provide many actions, a drop-down list displays the options. The actions that are available for the selected item appear in normal font, whereas those actions that are not available for the selected item are dimmed.
Filter	You can filter the table contents by a value that you enter.
Record count	The number of entries in the table.
Sort by column	You can sort all table entries by clicking on a column heading.
Table-specific toolbars	Toolbars are available for most tables, with options that are appropriate for the specific table.

Field Aids

includes the following aids to assist you in your tasks, whether configuring policies and profiles, troubleshooting faults, or looking for additional information for a particular window or dialog box.

Table 4: Field Aids

Feature	Description	Example
Tooltips	Pause your cursor over a field to view additional information about the field.	
Red field or box	Indicates that information is required. If you have entered information and the field remains red, the entry contains an error (such as an incomplete IP address). You can pause your mouse over the field to obtain information about the error.	

Feature	Description	Example
Field icons	Two field icons (i and c) provide additional information for the field: • The "i" icon provides additional information for the field. • The "c" icon identifies the feature support for the field. For example, a feature might be supported on ASA 1000Vs but not on VSGs. Pause your cursor over the icon to view the information.	
Fault links	Fault information and links to fault information are available for each edge and compute firewall in Resource Management. Navigate to a specific compute or edge firewall to view the object state, number of faults, and severity of faults. The same pane provides links to the relevant fault page.	
Online help	Context-sensitive online help is available for each pane and dialog box. To access help, click **Help** in the active pane or **?** in the active dialog box.	

Firewall Access

If the server is protected by a firewall, the following ports must be enabled:

- 22—TCP
- 80—HTTP
- 443—HTTPS
- 843—Adobe Flash
- 6644—TCP, UDP

Setting the Idle Timeout Period - Preferences

The Preferences dialog box allows you to specify the length of time, from 5 to 60 minutes, that a session on your current machine can remain idle before the session is closed. The value that you enter applies to the system that you used to log into .

Search

The Search tab enables you to search for instances of organizations in . From the search result, you can expand an organization's hierarchy and launch devices and polices in that organization.

Note Searching for organization names does not work if the organization names contain special characters.

SUMMARY STEPS

1. Do any of the following to launch the Search tab:
   - Choose **Policy Management > Service Policies > root > Search**.
   - Choose **Policy Management > Service Profiles > root > Search**.
   - Choose **Policy Management > Device Configurations > root > Search**.
   - Choose **Tenant Management > root > Search**.
   - Choose **Resource Management > Managed Resources > root > Search**.
2. Enter organization names as a *pattern or a regular expression.
   - To fetch organization names starting with "ABC", enter "ABC*".
   - To fetch organization names ending with "ABC", enter "*ABC".
   - To fetch organizations names starting with "A" and ending with "BC" but with other characters in between, enter "A*BC".
3. Click **Search**.

DETAILED STEPS

Step 1 Do any of the following to launch the Search tab:

- Choose **Policy Management > Service Policies > root > Search**.
- Choose **Policy Management > Service Profiles > root > Search**.
- Choose **Policy Management > Device Configurations > root > Search**.
- Choose **Tenant Management > root > Search**.
- Choose **Resource Management > Managed Resources > root > Search**.

Note You can perform the Search operation at any level in the organizational hierarchy.

Step 2 Enter organization names as a *pattern or a regular expression.
The Search feature is case-sensitive. When you enter a name as a regular expression, it can contain regex wildcards such as * , + , ? and so on. For example, "*" will match the previous character zero or more times. Searching myVdc* will return all names that contain "myVd" and "myVDC".

Use the following the guidelines when you enter a pattern:

- To fetch organization names starting with "ABC", enter "ABC*".
- To fetch organization names ending with "ABC", enter "*ABC".
- To fetch organizations names starting with "A" and ending with "BC" but with other characters in between, enter "A*BC".

Step 3 Click **Search**.
The search results are displayed in the table.

Clone

You can create a clone for an organization, policy, policy set, or profile at a destination of your choice. The hierarchy of an organization's clone or the names of the elements in it cannot be changed. After a clone is created, it cannot be renamed or moved to another location.

Note If you clone a policy set, such as a NAT policy set, the contained policies are not cloned. You must clone policies separately.

SUMMARY STEPS

1. Based on the element you want to clone, do one of the following:
   - To clone an organization, choose **Tenant Management > root > *tenant* > *organization***.
   - To clone a policy, policy set, or profile, choose **Policy Management > Service Polices > root > *tenant* > Policies > *policy*** or **Policy Management > Service Profiles > root > *tenant* > Profiles > *profile***.
2. Right-click the element to be cloned and choose **Clone**.
3. In the Clone dialog box that appears:

DETAILED STEPS

Step 1 Based on the element you want to clone, do one of the following:

- To clone an organization, choose **Tenant Management > root >** ***tenant*** **>** ***organization***.
- To clone a policy, policy set, or profile, choose **Policy Management > Service Polices > root >** ***tenant*** **> Policies >** ***policy*** or **Policy Management > Service Profiles > root >** ***tenant*** **> Profiles >** ***profile***.

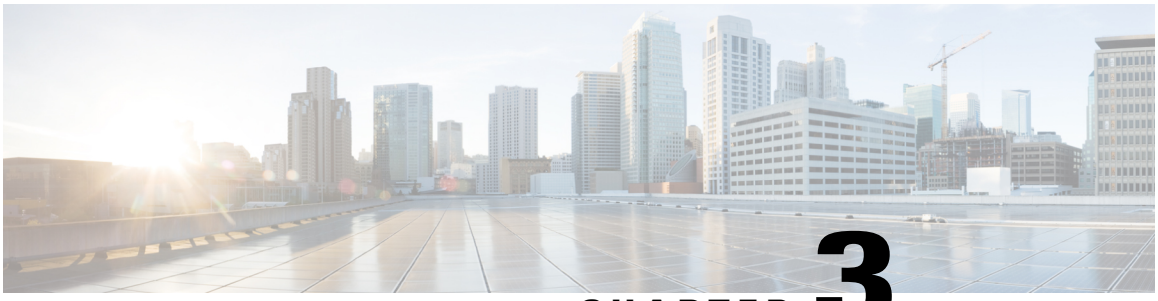
Step 2 Right-click the element to be cloned and choose **Clone**.

Step 3 In the Clone dialog box that appears:

a) Enter the name and destination of the clone.

b) Click **OK**.

The clone appears in the destination you chose.



CHAPTER 3

Configuring RBAC

This section contains the following topics:

- RBAC, page 13
- User Accounts, page 13
- User Roles, page 15
- Privileges, page 17
- User Locales, page 18
- Configuring User Roles, page 19
- Configuring User Locales, page 21
- Configuring Locally Authenticated User Accounts, page 24
- Monitoring User Sessions, page 28

RBAC

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 would be able to 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 would be able to 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

User accounts are used to access the system. Up to 260 local user accounts can be configured in each Prime Network Services Controller 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 or SECSH.

Default User Account

Each Prime Network Services Controller 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.

Username Guidelines

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

- The login ID can contain from 1 to 32 characters, including the following:
  - Any alphanumeric character
  - Period (.)
  - Underscore (_)
  - Dash (-)
  - At symbol (@)
- Neither the unique username nor a local user's username can consist solely of numbers.
- The unique username cannot start with a number.
- If an all-numeric username exists on a AAA server (LDAP) and is entered during login, 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 260 user accounts in a instance.

Password Guidelines

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 option is enabled, 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:
  - Lowercase letters
  - Uppercase letters
  - Digits
  - Special characters
- Must not contain a character that is repeated more than three 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 (?), or equals sign (=).
- Should not be blank for local user and admin accounts.

Note The Password Strength Check option is enabled by default. You can disable it from the Locally Authenticated Users pane (Administration > Access Control > Locally Authenticated Users).

Note If 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 for authentication only, not authorization. The definition of the local user role definition applies to the remotely authenticated user.

User Roles

A user role contains one or more privileges that define the operations allowed for the user who is assigned to that 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 instance. The difference between the read-only role and other roles is that a user who is assigned only 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

Users have read and write access to users, roles, and AAA configuration, and read access to the rest of the system.

admin

Users have read and write access to the entire system and has most privileges. However, users cannot create or delete files, or perform system upgrades. These functions can be done only through the default admin account. The default admin account is assigned this role by default, and it cannot be changed.

intercloud-infra

Users have read and write access for InterCloud operations, including creating InterCloud links, creating provider accounts, managing InterCloud Extender and Switch images, and importing InterCloud Agent images. Users with this role are limited to InterCloud functionality.

intercloud-server

Users have read and write access for cloud VMs. User can create or move VMs from the enterprise to the cloud. Users can monitor cloud VMs for multiple tenants. Users with this role are limited to InterCloud functionality.

network

Users can create organizations, security policies, and device profiles.

operations

Users can acknowledge faults, back up the system, and perform some basic operations, such as logging configuration.

read-only

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

tenant-admin

Users can configure tenant-related policies and resources for their associated tenants. However, users can view only those objects related to their associated tenants as defined by their assigned locales and organizations. They cannot see information about tenants that do not belong to their assigned locales and organizations.

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

- Role
- Privilege for a role
- Locale
- Organization in a locale

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.
InterCloud-Infrastructure	(Internal use) InterCloud infrastructure management.
InterCloud-Server	InterCloud VM management.
read-only	Read-only access. Read-only cannot be selected as a privilege; it is assigned to every user role.
Resource Configuration	Service device configuration.
Policy Management	Service device policies.
Fault Management	Alarms and alarm policies.
Operations	Logs, core file management, system backup, 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 roles and the associated privileges.

Role	Associated Privileges
aaa	aaa
admin	admin
intercloud-infra	InterCloud-Infrastructure
intercloud-server	InterCloud-Server
network	policy, res-config, tenant

Role	Associated Privileges
operations	fault, operations
read-only	read-only
tenant-admin	policy, res-config, tenant

User Locales

A user can be assigned one or more locales. Each locale specifies one or more organizations or 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 organizations when creating policies. One exception to this rule is a locale with root as the associated organization, 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.

At least one locale is required when adding a user account with either the network or tenant-admin role. If all the locales associated with a tenant-admin or network user are deleted, the tenant-admin or network user will not have access to the system. A user with the admin role needs to manually delete the user.

Note Users not assigned to a locale have access to all resources in all organizations. For users assigned to a locale, access is restricted to the objects that reside under the organizations that belong to that locale.

Users with AAA privileges (AAA 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 to that locale can assign only the Engineering organization to other users.

Note AAA privileges must be carefully assigned because they allow a user to manage other users' privileges and role assignments.

You can hierarchically manage organizations. A user who is assigned to 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 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 assignments for a local user can be changed on . The role and locale for a remote user can be changed on LDAP. If any of the following information assigned to a user is modified, the administrator must delete all existing sessions of that user so that the new privileges take effect:

- Role
- Privilege for a role

- Locale
- Organization in a locale

Configuring User Roles

Creating a User Role

SUMMARY STEPS

1. Choose **Administration > Access Control > Roles**.
2. Click **Create Role**.
3. In the Create Role dialog box, complete the following fields, then click **OK**:

DETAILED STEPS

Step 1 Choose **Administration > Access Control > Roles**.

Step 2 Click **Create Role**.

Step 3 In the Create Role dialog box, complete the following fields, then click **OK**:

Field	Description
Name	User role name.
Privileges	Available privileges. To assign a privilege to the selected role, check one or more of the following check boxes: • Admin • AAA • Fault Management • InterCloud-Infrastructure • InterCloud-Server • Operations • Policy Management • Resource Configuration • Tenant Management You can assign the admin privilege, which includes all privileges, or you can assign privileges individually.

Editing a User Role

SUMMARY STEPS

1. Choose **Administration > Access Control > Roles**.
2. Select the role you want to edit, then click **Edit**.
3. In the Edit dialog box, check or uncheck the boxes for the privileges you want to add to or remove from the role, then click **OK**.

DETAILED STEPS

Step 1 Choose **Administration > Access Control > Roles**.

Step 2 Select the role you want to edit, then click **Edit**.

Step 3 In the Edit dialog box, check or uncheck the boxes for the privileges you want to add to or remove from the role, then click **OK**.

Deleting a User Role

Except for the admin and read-only roles, you can delete user roles that are not appropriate for your environment.

SUMMARY STEPS

1. Choose **Administration > Access Control > Roles**.
2. Select the user role you want to delete, then click **Delete**.
3. In the Confirm dialog box, click **Yes**.

DETAILED STEPS

Step 1 Choose **Administration > Access Control > Roles**.

Step 2 Select the user role you want to delete, then click **Delete**.

Note You cannot delete the admin or read-only role.

Step 3 In the Confirm dialog box, click **Yes**.

Configuring User Locales

Creating a Locale

Before You Begin

Verify that one or more tenants exist; if none exist, create one. For information on creating tenants, see Creating a Tenant, on page 67.

SUMMARY STEPS

1. Choose **Administration > Access Control > Locales**.
2. Click **Create Locale**.
3. In the Create Locale dialog box, complete the following fields, then click **OK**:

DETAILED STEPS

Step 1 Choose **Administration > Access Control > Locales**.

Step 2 Click **Create Locale**.

Step 3 In the Create Locale dialog box, complete the following fields, then click **OK**:

Field	Description
Name	Locale name, containing 2 to 255 characters. The name can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:). You cannot change this name after it is saved.
Description	Brief locale description, containing 1 to 256 characters. The description can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:).
Assigned Organizations	
Assign Organization	Click to assign organizations to locales.
Assigned Organization	List of organizations assigned to the locale.

What to Do Next

Add the locale to one or more user accounts. For more information, see Changing the Locales or Roles Assigned to a Locally Authenticated User, on page 28.

Editing a Locale

SUMMARY STEPS

1. Choose **Administration > Access Control > Locales**.
2. In the list of locales, select the locale you want to edit, then click **Edit**.
3. In the Description field, change the description as appropriate.
4. Click **Assign Organization**.
5. In the Assign Organization dialog box:
6. Click **OK** in the open dialog boxes to save your changes.

DETAILED STEPS

Step 1 Choose **Administration > Access Control > Locales**.

Step 2 In the list of locales, select the locale you want to edit, then click **Edit**.

Step 3 In the Description field, change the description as appropriate.

Step 4 Click **Assign Organization**.

Step 5 In the Assign Organization dialog box:

a) Expand the root node to view the available organizations.

b) Check the check boxes of the organizations to assign to the locale.

Step 6 Click **OK** in the open dialog boxes to save your changes.

Deleting a Locale

Before You Begin

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

Note If all the locales associated with a tenant-admin or network user are deleted, the tenant-admin or network user will not have access to the system. A user with the admin role needs to manually delete the user.

SUMMARY STEPS

1. Choose **Administration** > **Access Control** > **Locales**.
2. In the pane, click the locale you want to delete, and then click **Delete**.

DETAILED STEPS

Step 1 Choose **Administration** > **Access Control** > **Locales**.

Step 2 In the pane, click the locale you want to delete, and then click **Delete**.

Assigning an Organization to a Locale

SUMMARY STEPS

1. Choose **Administration > Access Control > Locales >** *locale*, then click **Assign Organization**.
2. In the Assign Organization dialog box:
3. Click **OK** in the open dialog boxes, then click **Save** to save the locale.

DETAILED STEPS

Step 1 Choose **Administration > Access Control > Locales >** *locale*, then click **Assign Organization**.

Step 2 In the Assign Organization dialog box:

a) Expand root to view the available organizations.

b) Check the check boxes for the organizations you want to add to the locale.

Step 3 Click **OK** in the open dialog boxes, then click **Save** to save the locale.

Deleting an Organization from a Locale

SUMMARY STEPS

1. Choose **Administration > Access Control > Locales >** *locale*.
2. In the content pane, click the **General** tab.
3. In the Assigned Organizations area, select the organization you want to delete, then click **Delete Organization**.
4. When prompted, confirm the deletion, then click **Save**.

DETAILED STEPS

Step 1 Choose **Administration > Access Control > Locales >** *locale*.
Step 2 In the content pane, click the **General** tab.
Step 3 In the Assigned Organizations area, select the organization you want to delete, then click **Delete Organization**.
Step 4 When prompted, confirm the deletion, then click **Save**.

Configuring Locally Authenticated User Accounts

Creating a User Account

When you create a user account, you assign one or more roles to the account. If you assign either the network or tenant-admin role to a user, you must also assign a locale. For information on creating locales, see Creating a Locale, on page 21.

Before You Begin

Configure locales for accounts that will require either the network or tenant-admin role.

SUMMARY STEPS

1. Choose **Administration > Access Control > Locally Authenticated Users**.
2. Click **Create Locally Authenticated Users**.
3. In the **Properties** area, complete the following fields:
4. In the **Roles/Locales** tab area, complete the following fields:
5. In the **SSH** tab area, complete the following fields, and then click **OK**:

DETAILED STEPS

Step 1 Choose **Administration > Access Control > Locally Authenticated Users**.
Step 2 Click **Create Locally Authenticated Users**.
Step 3 In the **Properties** area, complete the following fields:

Field	Description
Login ID	Login name. This name must be unique and meet the following guidelines and restrictions for user accounts: • The login ID can be between 1 and 32 characters, including the following: ◦ Any alphanumeric character ◦ Underscore (_) ◦ Dash (-) ◦ At symbol (@) • 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.
Description	User description.
First Name	User first name. This field can contain up to 32 characters.
Last Name	User last name. This field can contain up to 32 characters.
Email	User email address.
Phone	User telephone number.

Field	Description
Password	Password associated with this account. For maximum security, each password must be strong. If the Password Strength Check check box is checked, the system rejects any password that does not meet the following requirements: • Contains a minimum of eight characters • Contains at least three of the following: ◦ Lowercase letters ◦ Uppercase letters ◦ Digits ◦ Special characters • Does not contain a character that is repeated more than three times consecutively, such as aaabbb. • Is not the user name or the reverse of the user name. • Passes a password dictionary check. For example, the password must not be based on a standard dictionary word. • Does not contain the following symbols: dollar sign ($), question mark (?), equals sign (=). • The password must not be blank for local user and admin accounts. **Note** The password strength check box on the Locally Authenticated Users pane can be unchecked, indicating that the password is not required to be strong. It must, however, contain a minimum of eight characters. The password field is a required field, and a user cannot be created without providing a password.
Confirm Password	Reenter the password for confirmation purposes.
Password Expires	Indicates whether or not password expiration is enabled. Check the check box to enable password expiration. If you enable password expiration, the following occurs when the expiration date is reached: • The account is disabled. • The user cannot log in or reset their password. A user with administrator privileges must extend the expiration date before the user can log in again. The user cannot change their password.
Expiration Date	Available if password expiration is enabled. Date that the password expires.

Step 4 In the **Roles/Locales** tab area, complete the following fields:

Field	Description
Assigned Roles	Check the applicable check boxes to assign one or more roles to the user: **Note** You must assign a locale to a user before you can assign the network or tenant-admin role. • aaa • admin • intercloud-infra • intercloud-server • network • operations • read-only • tenant-admin
Assigned Locale	Check the applicable check boxes to assign one or more locales to the user. **Note** You must assign a locale to a user before you can assign the network or tenant-admin role.

Step 5 In the **SSH** tab area, complete the following fields, and then click **OK**:

Field	Description
Key	SSH key. If you choose the Key radio button, the SSH Data field is displayed.
Password	SSH password.
SSH Data	Available if Key is selected. Enter the SSH public key.

Changing the Locales or Roles Assigned to a Locally Authenticated User

SUMMARY STEPS

1. Choose **Administration > Access Control > Locally Authenticated Users >** *user*.
2. In the General tab, click the **Roles/Locales** tab.
3. Check or uncheck the appropriate check boxes to assign or remove a locale or role then click **Save**.

DETAILED STEPS

Step 1 Choose **Administration > Access Control > Locally Authenticated Users >** *user*.

Step 2 In the General tab, click the **Roles/Locales** tab.

Step 3 Check or uncheck the appropriate check boxes to assign or remove a locale or role then click **Save**.

Monitoring User Sessions

You can monitor sessions for both locally and remotely authenticated users.

SUMMARY STEPS

1. Choose **Administration > Access Control**, then choose one of the following:
   - **Locally Authenticated Users >** *user*.
   - **Remotely Authenticated Users >** *user*.
2. Click the **Sessions** tab to view the user session.

DETAILED STEPS

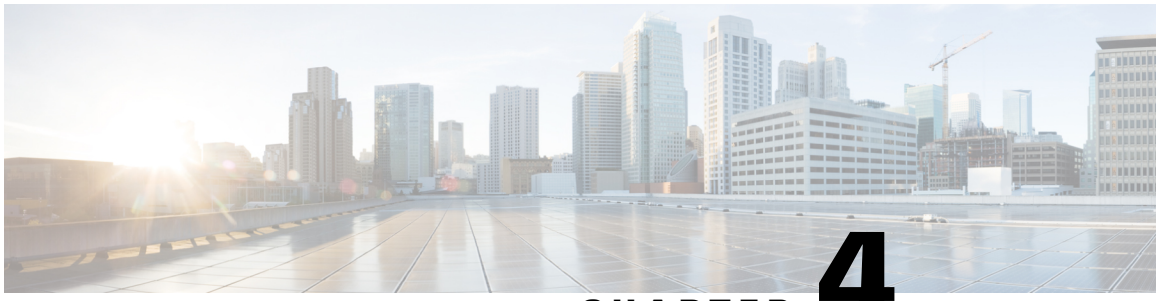
Step 1 Choose **Administration > Access Control**, then choose one of the following:

- **Locally Authenticated Users >** *user*.
- **Remotely Authenticated Users >** *user*.

Step 2 Click the **Sessions** tab to view the user session.

Field	Description
Host	IP address from which the user logged in.
Login Time	Date and time that the user logged in.

Field	Description
UI	User interface for this session: • web—GUI login • shell—CLI login • ep—End point
Terminal Type	Kind of terminal through which the user is logged in.



CHAPTER 4

Configuring Primary Authentication

This section includes the following topics:

- Primary Authentication, page 31
- Remote Authentication Providers, page 31
- Creating an LDAP Provider, page 32
- Editing an LDAP Provider, page 34
- Deleting an LDAP Provider, page 35
- Selecting a Primary Authentication Service, page 35

Primary Authentication

supports two methods to authenticate user logins:

- Local to
- Remote through LDAP

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

- Role
- Privilege for a role
- Locale
- Organization in a locale

Remote Authentication Providers

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

User Accounts in Remote Authentication Services

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

The temporary sessions for users who log in through remote authentication services can be viewed through the 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 and that the names of those roles and locales match the names used in . If an account does not have the required roles and locales, the user is granted only read-only privileges.

LDAP Attribute for User

In , the LDAP attribute that holds the LDAP user roles and locales is preset. This attribute 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, 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 starts 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 . You can use an existing LDAP attribute that is mapped to the user roles and locales, or you can 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).

SUMMARY STEPS

1. Choose **Administration > Access Control > LDAP**.
2. In the content pane, click **Create LDAP Provider**.
3. In the Create LDAP Provider dialog box, provide the following information: then click **OK** and **Save**.

DETAILED STEPS

Step 1 Choose **Administration > Access Control > LDAP**.

Step 2 In the content pane, click **Create LDAP Provider**.

Step 3 In the Create LDAP Provider dialog box, provide the following information: then click **OK** and **Save**.

Field	Description
Hostname/IP Address	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 instead of an IP address, you must configure a DNS server in the server.
Key	Password for the LDAP database account specified in the Root DN field. The maximum is 32 characters.
Root DN	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 127 characters.
Port	Port through which communicates with the LDAP database. The default port number is 389.
Enable SSL	Check to enable SSL.

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 35.

Editing an LDAP Provider

SUMMARY STEPS

1. Choose **Administration > Access Control > LDAP** > *ldap-adapter*, then click **Edit**.
2. In the Edit dialog box, modify the settings as as described in the following table, then click **OK** and **Save**.

DETAILED STEPS

Step 1 Choose **Administration > Access Control > LDAP** > *ldap-adapter*, then click **Edit**.

Step 2 In the Edit dialog box, modify the settings as as described in the following table, then click **OK** and **Save**.

Field	Description
Name	Hostname or IP address of the LDAP provider (read-only). 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 instead of an IP address, you must configure a DNS server in the server.
Key	Password for the LDAP database account specified in the Root DN field. The maximum is 32 characters.
Set	Whether or not the preshared key has been set and is properly configured (read-only). If the Set value is Yes, and the Key field is empty, it indicates that a key was provided previously.
Root DN	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 127 characters.
Port	Port through which communicates with the LDAP database. The default port number is 389.
Enable SSL	Check to enable SSL.

Deleting an LDAP Provider

SUMMARY STEPS

1. Choose **Administration > Access Control > LDAP >***ldap-provider*, then click **Delete**.
2. Confirm the deletion, then click **Save**.

DETAILED STEPS

Step 1 Choose **Administration > Access Control > LDAP >***ldap-provider*, then click **Delete**.

Step 2 Confirm the deletion, then click **Save**.

Selecting a Primary Authentication Service

Note If the default authentication is set to LDAP, and the LDAP servers are not operating or are unreachable, the local admin user can log in at any time and make changes to the authentication, authorization, and accounting (AAA) system.

SUMMARY STEPS

1. Choose **Administration > Access Control > Authentication**.
2. In the Properties tab, specify the information as described in the following table, then click **OK**.

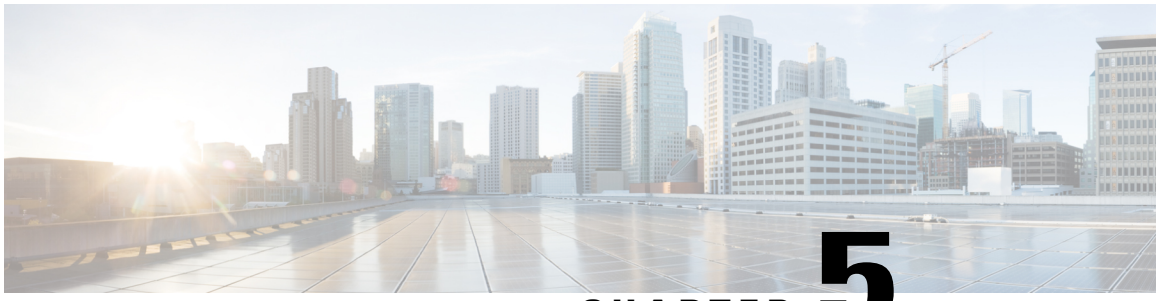
DETAILED STEPS

Step 1 Choose **Administration > Access Control > Authentication**.

Step 2 In the Properties tab, specify the information as described in the following table, then click **OK**.

Field	Description
Default Authentication	Default method by which a user is authenticated during remote login: • LDAP—The user must be defined on the LDAP server specified for this instance. • Local—The user must be defined locally in this instance. • None—A password is not required when the user logs in remotely.

Field	Description
Role Policy to Remote Users	Action taken when a user attempts to log in and the LDAP server does not supply a user role with the authentication information: • assign-default-role—The user can log in with a read-only user role. • no-login—The user cannot log into the system, even if the user name and password are correct.



CHAPTER 5

Configuring Trusted Points

This section includes the following topics:

- Trusted Points, page 37
- Configuring Trusted Points, page 37

Trusted Points

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

- The certificate of the certificate authority (CA) that issued the LDAP server certificate.
- If the 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

SUMMARY STEPS

1. Choose **Administration > Access Control > Trusted Point**, then click **Create Trusted Point**.
2. In the Create Trusted Point dialog box, complete the following fields, then click **OK**.

DETAILED STEPS

Step 1 Choose **Administration > Access Control > Trusted Point**, then click **Create Trusted Point**.

Step 2 In the Create Trusted Point dialog box, complete the following fields, then click **OK**.

Field	Description
Name	Trusted point name.
Certificate Chain	Certificate information for this trusted point.

Editing a Trusted Point

SUMMARY STEPS

1. Choose **Administration > Access Control > Trusted Point**, then click **Edit**.
2. In the Edit dialog box, modify the certificate chain as appropriate, then click **OK**.

DETAILED STEPS

Step 1 Choose **Administration > Access Control > Trusted Point**, then click **Edit**.

Step 2 In the Edit dialog box, modify the certificate chain as appropriate, then click **OK**.
The Name and Fingerprint fields cannot be modified.

Deleting a Trusted Point

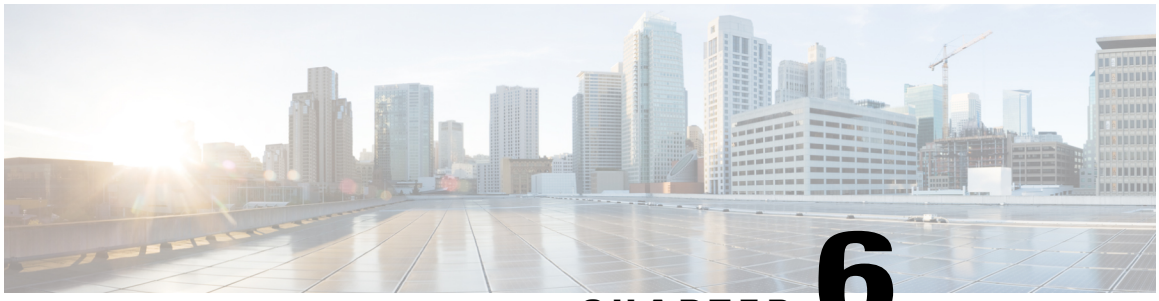
SUMMARY STEPS

1. Choose **Administration > Access Control > Trusted Point >** *trusted-point*, then click **Delete**.
2. When prompted, confirm the deletion.

DETAILED STEPS

Step 1 Choose **Administration > Access Control > Trusted Point >** *trusted-point*, then click **Delete**.

Step 2 When prompted, confirm the deletion.



CHAPTER 6

Configuring VM Managers

This section includes the following topics:

- VM Manager Overview, page 39
- Hypervisor and VMM Support, page 40
- Configuring Connectivity with VMware vCenter, page 41
- Configuring Connectivity with Microsoft SCVMM, page 44
- Editing a VM Manager, page 45
- Deleting a VM Manager, page 47

VM Manager Overview

After you install on a hypervisor, you must configure so that it can communicate with the Virtual Machine Manager (VMM) for that hypervisor and the VMs that manages.

Note Hypervisors Openstack KVM and Microsoft HyperV are supported up to PNSC release 3.4.1d.

communicates with the VMM to perform the following actions on the VMs that manages:

- Obtain the VM attributes that uses to define security or service policies for Nexus 1000V switches, VSG compute firewalls, and CSR 1000V edge routers.
- Instantiate, start, stop, restart, or delete VMs.
- Map VM network interfaces.
- Instantiate and configure services on service VMs.

For information on configuring VMM connectivity, see the following topics:

- Configuring Connectivity with VMware vCenter, on page 41
- Configuring Connectivity with Microsoft SCVMM, on page 44

Note You must reestablish connectivity with the VMM if you change the server hostname or fully qualified domain name (FQDN).

Hypervisor and VMM Support

supports hypervisors and their VMMs as follows:

- VMware ESX with vCenter—All functionality described in VM Manager Overview, on page 39.
- Microsoft Hyper-V with SCVMM—Only read attributes and configure VSG compute firewalls.

Note No other VMMs are supported for managing VMs hosted by VMware ESX or Hyper-V Hypervisor. Although SCVMM can communicate with VMs configured on a VMware ESX hypervisor, support is restricted to homogeneous environments. That is, you can use SCVMM only with Hyper-V Hypervisor and vCenter only with VMware ESX.

Note SCVMM is supported till PNSC version 3.4.1d.

The following table identifies the differences between the supported hypervisors with regard to Prime Network Services Controller features and devices. Other features and devices that Prime Network Services Controller supports but that are not listed in the table are expected to perform consistently on both hypervisors with their respective VMMs.

Table 5: Hypervisors and Prime Network Services Controller Feature Support

Feature	VMware ESX with vCenter	Microsoft Hyper-V Hypervisor with SCVMM
Network attributes	All	All
VM attribute support	Supported: • Cluster name • Guest OS full name • Hypervisor name • Parent application name • Port profile name • Resource pool • VM DNS name • VM name	Supported: • Guest OS full name • Port profile name • VM DNS name • VM name

Feature	VMware ESX with vCenter	Microsoft Hyper-V Hypervisor with SCVMM
VM Refresh button	Not supported	Supported
Device and Feature Support		
ASA 1000V	Supported	Not supported
Citrix NetScaler load balancer	Supported (ESXi)	Not supported
CSR 1000V	Supported	Not supported
Integration with DCNM	Supported (ESXi)	Not supported
InterCloud functionality	Supported	Not supported
VSG	Supported	Supported

Configuring Connectivity with VMware vCenter

Establish connectivity between and VMware vCenter by performing the following tasks:

1 Exporting the vCenter Extension File, on page 41

2 Registering the vCenter Extension Plugin in vCenter, on page 42

3 Configuring Connectivity with vCenter, on page 43

Note You need to export and Register the VMware vCenter Extension plugin for VMware vCenter releases 5.5 and 6.0. For VMware vCenter release 6.5 onward, plugin registration is automated and you need to enter VMware vCenter Administrator Credentials while adding VM Manager.

Exporting the vCenter Extension File

The first step in configuring connectivity with VMware vCenter is exporting the vCenter extension file.

Before You Begin

If you use Internet Explorer, do one of the following to ensure that you can download the extension file:

- Open Internet Explorer in Administrator mode.
- After starting Internet Explorer, choose **Tools > Internet Options > Security**, and uncheck the **Enable Protected Mode** check box.

SUMMARY STEPS

1. In , choose **Resource Management > VM Managers > VM Managers**.
2. In the VM Managers pane, click **Export vCenter Extension**.
3. Save the vCenter extension file in a directory that the vSphere Client can access because you will need to register the vCenter extension plug-in from within the vSphere Client (see Registering the vCenter Extension Plugin in vCenter, on page 42).
4. Open the XML extension file to confirm that the content is available.

DETAILED STEPS

Step 1 In , choose **Resource Management > VM Managers > VM Managers**.

Step 2 In the VM Managers pane, click **Export vCenter Extension**.

Step 3 Save the vCenter extension file in a directory that the vSphere Client can access because you will need to register the vCenter extension plug-in from within the vSphere Client (see Registering the vCenter Extension Plugin in vCenter, on page 42).

Step 4 Open the XML extension file to confirm that the content is available.

Registering the vCenter Extension Plugin in vCenter

Registering the vCenter extension plug-in enables you to create a VM Manager in Prime Network Services Controller and communicate with the vCenter VMM and the VMs that Prime Network Services Controller manages.

SUMMARY STEPS

1. From the VMware vSphere Client, log in to the vCenter server that you want to manage by using Prime Network Services Controller.
2. In the vSphere Client, choose **Plug-ins > Manage Plug-ins**.
3. Right-click the window background and choose **New Plug-in**.
4. Browse to the Prime Network Services Controller vCenter extension file that you previously exported and click **Register Plug-in**.
5. In the security warning message box, click **Ignore**.
6. When the success message is displayed, click **OK**, and then click **Close**.

DETAILED STEPS

Step 1 From the VMware vSphere Client, log in to the vCenter server that you want to manage by using Prime Network Services Controller.

Step 2 In the vSphere Client, choose **Plug-ins > Manage Plug-ins**.

Step 3 Right-click the window background and choose **New Plug-in**.

Tip Scroll down and right-click near the bottom of the window to view the New Plug-in option.

Step 4 Browse to the Prime Network Services Controller vCenter extension file that you previously exported and click **Register Plug-in**.
The vCenter Register Plug-in window appears, displaying a security warning.

Step 5 In the security warning message box, click **Ignore**.
Note If desired, you can install this certificate for further integration with Public Key Infrastructure (PKI) and Kerberos facilities.
A progress indicator shows the task status.

Step 6 When the success message is displayed, click **OK**, and then click **Close**.

Configuring Connectivity with vCenter

After you register the vCenter extension plug-in in vCenter, you can configure connectivity with vCenter in Prime Network Services Controller.

SUMMARY STEPS

1. Choose **Resource Management > VM Managers > VM Managers**, and then click **Add VM Manager**.
2. In the Add VM Manager dialog box, enter the following information and then click **OK**:

DETAILED STEPS

Step 1 Choose **Resource Management > VM Managers > VM Managers**, and then click **Add VM Manager**.

Step 2 In the Add VM Manager dialog box, enter the following information and then click **OK**:

- Name—VMM name.
- Description—VMM description.
- Hostname / IP Address—Hostname or IP address of the VMM.
- Port Number—Port number to use for communications.
- For VMware vCenter release 6.5, choose **vCenter 6.5 and greater** check box and enter vSphere vCenter Administrator credentials.

A successfully added VMM is displayed with the following information:

- Admin State of *enable*.
- Operational State of *up*.
- VMware vCenter version.

Configuring Connectivity with Microsoft SCVMM

Use this procedure to configure connectivity with Microsoft SCVMM (SCVMM).

Note SCVMM is supported up to Cisco PNSC version 3.4.1d.

Before You Begin

- Confirm that you have the username and password for SCVMM access.
- Install Microsoft Service Provider Framework (SPF) so that can communicate with SCVMM. For more information, see http://technet.microsoft.com/en-us/library/jj642895.aspx.
- Confirm that SPF is installed correctly and functional in SCVMM by connecting to https://spf_host_ip:8090/SC2012R2/VMM/Microsoft.Management.Odata.Svc.

SUMMARY STEPS

1. Choose **Resource Management > VM Managers**, and then click **Add VM Manager**.
2. In the Add VM Manager dialog box, provide the information described in the following table, and then click **OK**:

DETAILED STEPS

Step 1 Choose **Resource Management > VM Managers**, and then click **Add VM Manager**.

Step 2 In the Add VM Manager dialog box, provide the information described in the following table, and then click **OK**:

Field	Description
Name	VMM name.
Description	VMM description.
Hostname / IP Address	Hostname or IP address of the VMM.
Domain Name / Username	Domain or username for SCVMM access.
Password	Password for SCVMM access.
Port Number	Port to use for communications.

A successfully added VMM is displayed with the following information:

- Admin State of *enable*.

- Operational State of *up*.
- SCVMM version.

Editing a VM Manager

Openstack KVM and Microsoft HyperV hypervisors are supported on Cisco PNSC up to release 3.4.1d. After a VM Manager is added, you can modify its properties as follows:

- Admin State—For vCenter and SCVMM.
- Description—For vCenter and SCVMM.
- Domain Name / Username—SCVMM only.
- Password—SCVMM only.

All other fields are read-only.

Changing the administrative state depends on the current operational state:

- To change the administrative state to enabled, the operational state must be down.
- To change the administrative state to disabled, the operational state must be up.

If your request to change the administrative state fails, resubmit the request when the system has the correct operational state.

Note SCVMM is supported up to Cisco PNSC version 3.4.1d.

SUMMARY STEPS

1. Choose one of the following:
   - **Resource Management > VM Managers**
   - **InterCloud Management > Enterprise > VM Managers**
2. In the VM Managers tab, select the VM Manager you want to edit, and then click **Edit**.
3. In the Edit VM Manager dialog box, edit the information as required, and then click **OK**.

DETAILED STEPS

Step 1 Choose one of the following:
- **Resource Management > VM Managers**
- **InterCloud Management > Enterprise > VM Managers**

Step 2 In the VM Managers tab, select the VM Manager you want to edit, and then click **Edit**.

Step 3 In the Edit VM Manager dialog box, edit the information as required, and then click **OK**.

Field	Description
Name	VM Manager (VMM) name (read-only).
Description	Description of the VMM.
Hostname / IP Address	Hostname or IP address of the VMM (read-only). For OpenStack, this is the hostname or IP address of the OpenStack controller.
Service Tenant	Name of the OpenStack project that was created for network services and the management network.
Domain Name / Username	(SCVMM and OpenStack) Domain or username for hypervisor access. For OpenStack, the admin or superuser username.
Password	(SCVMM only) Password for SCVMM access.
Port Number	Port used for communications (read-only). For OpenStack, the port number of the Keystone service running on the OpenStack controller.
Admin State	One of the following administrative states for the VMM: • enable—When a VMM is added to with the administrative state of enable, the system fetches all VM inventory from the VMM. Any changes that occur to the VM on the VMM are also fetched. • disable—When a VMM is added to with the administrative state of disable, the system displays all discovered VMs from the VMM. Any changes that occur to the VMs on the VMM are not fetched. The changes will be fetched by when the admin state is changed to enable.
Type	VMM vendor (read-only).
Version	VMM version (read-only). A version is not displayed for OpenStack KVM.
Operational State	One of the following operational states (read-only): • up • unreachable • bad-credentials • comm-err • admin-down • unknown

Field	Description
Operational State Reason	Reason for the operational state (read-only).

Deleting a VM Manager

You cannot delete a VM Manager if a service VM is deployed on the associated VMM.

SUMMARY STEPS

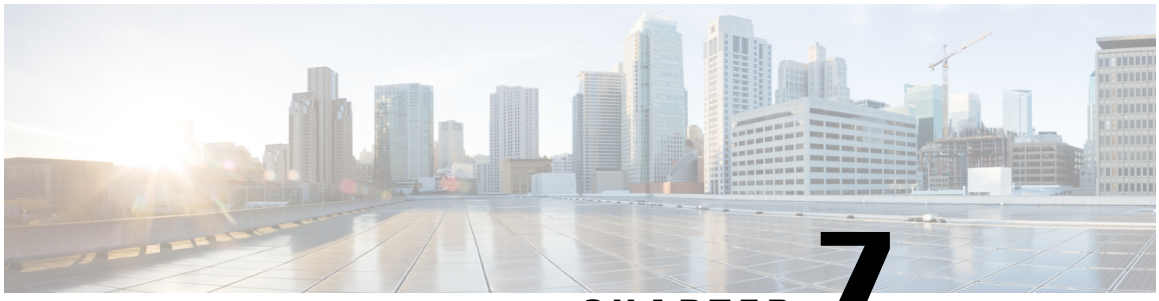
1. Choose one of the following:
   - **Resource Management > VM Managers**
   - **InterCloud Management > Enterprise > VM Managers**
2. Choose the VM Manager that you want to delete, and then click **Delete**.
3. When prompted, confirm the deletion.

DETAILED STEPS

Step 1 Choose one of the following:
- **Resource Management > VM Managers**
- **InterCloud Management > Enterprise > VM Managers**

Step 2 Choose the VM Manager that you want to delete, and then click **Delete**.

Step 3 When prompted, confirm the deletion.



CHAPTER 7

Configuring System Profiles

This section includes the following topics:

- System Profile Overview, page 49
- Policies in Profiles, page 49
- Configuring Policies, page 50
- Modifying the Default Profile, page 60
- Editing a DNS Domain, page 62
- Adding an NTP Server, page 62

System Profile Overview

provides one default System profile. The System profile includes time zone, DNS domain, DNS Server and NTP Server IP address information that is automatically generated using the data taken from initial installation. The System profile also contains the following policies: log file, fault, syslog, and core file. You can add and modify DNS server, NTP server, and policy information associated to the default system profile. However, you cannot create a new DNS domain or delete the default System profile.

Note

- Access to a DNS server and an NTP server is required for to communicate with the Amazon Cloud Provider.
- If you change the fully qualified domain name (FQDN), you must reconfigure connectivity with the hypervisor.

Policies in Profiles

You can create multiple policies and assign them to the System profile. To manage policies for the default System profile, choose **Administration > System Profile**.

Note The system profile uses name resolution to resolve policy assignments. For details, see Name Resolution in a Multi-Tenant Environment, on page 66.

The following policies, which are created under root, are visible in the System profile:

- Core file
- Fault
- Log file
- Syslog

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

Note You cannot delete existing default policies.

Configuring Policies

Configuring a Core File Policy Profile

You can create and modify the core file policy attributes. For more information on core file policy attributes, see the Core File Attributes Table.

To add, modify, or delete a core file policy:

SUMMARY STEPS

1. Choose **Administration > Profile > root > Policies > Core File**.
2. In the General tab, do one of the following:

DETAILED STEPS

Step 1 Choose **Administration > Profile > root > Policies > Core File**.

Step 2 In the General tab, do one of the following:

- To add a core file policy, click **Add Core File Policy**. Enter the appropriate information and click **OK**
- To edit a core file policy, select the policy, and then click **Edit**. Edit the appropriate fields and click **OK**.
- To delete a core file policy, select the policy, and then click **Delete**.

Core File Attributes Table

Field	Description
Name	Core file policy name, containing 1 to 32 characters. You can use alphanumeric characters, hyphen (-), underscore (_), and period (.). You cannot change the name after the policy has been saved.
Description	Brief policy description, containing 1 to 256 characters. You can use alphanumeric characters, hyphen (-), underscore (_), and period (.).
Admin State	Indicate whether the administrative state of the policy is to be enabled or disabled.
Hostname/IP Address	Hostname or IP address to use for this policy. If you use a hostname rather than an IP address, you must configure a DNS server in .
Port	Port number for sending the core dump file.
Protocol	Protocol for exporting the core dump file (tftp only).
Path	Path to use when storing the core dump file on a remote system. The default path is /tftpboot; for example, /tftpboot/*test*, where *test* is the subfolder.

Configuring a Fault Policy

When the system boots up, a default fault policy is created. You can add additional fault policies or modify existing ones. However, you cannot delete the default fault policy. For more information on fault policy attributes, see the Fault Policy Attributes Table.

To add, modify, or delete a fault policy:

SUMMARY STEPS

1. Choose **Administration > Profile > root > Policies > Fault**.
2. In the General tab, do one of the following:

DETAILED STEPS

Step 1 Choose **Administration > Profile > root > Policies > Fault**.

Step 2 In the General tab, do one of the following:

- To add a fault file policy, click **Add Fault File Policy**. Enter the appropriate information and click **OK**
- To edit a fault file policy, select the policy, and then click **Edit**. Edit the appropriate fields and click **OK**.
- To delete a fault file policy, select the policy, and then click **Delete**.

Fault Policy Attributes Table

Field	Description
Name	Fault policy name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, period, and colon. You cannot change this name after it is created.
Description	Brief policy description.
Flapping Interval	Length of time (in hours, minutes, and seconds) that must elapse before the system allows a fault to change its state. 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 default flapping interval is ten seconds.
Clear Faults Retention Action	Action to be taken when faults are cleared: • retain—Retain the cleared faults. • delete—Delete fault messages as soon as they are marked as cleared.
Clear Faults Retention Interval	How long the system is to retain cleared fault messages: • Forever—The system retains all cleared fault messages regardless of their age. • Other—The system retains cleared fault message for a specified the length of time. In the spinbox that is displayed when you select this option, enter the length of time (in days, hours, minutes, and seconds) that the system is to retain cleared fault messages.

Configuring a Logging Policy

When the system boots up, a default logging policy is created. You can add additional log policies or modify existing ones. However, you cannot delete the default log policy. For more information on logging policy attributes, see the Logging Policy Attributes Tables.

SUMMARY STEPS

1. Choose **Administration > Profile > root > Policies > Log File**.
2. In the General tab, do one of the following:

DETAILED STEPS

Step 1 Choose **Administration > Profile > root > Policies > Log File**.

Step 2 In the General tab, do one of the following:

- To add a logging file policy, click **Add Logging File Policy**. Enter the appropriate information and click **OK**
- To edit a logging file policy, select the policy, and then click **Edit**. Edit the appropriate fields and click **OK**.
- To delete a logging file policy, select the policy, and then click **Delete**.

Logging Policy Attributes Tables

Field	Description
Name	Logging policy name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, period, and colon. You cannot change this name after it is created.
Description	Brief policy description.

Field	Description
Log Level	One of the following logging severity levels: • debug0 • debug1 • debug2 • debug3 • debug4 • info • warning • minor • major • critical The default log level is info.
Backup Files Count	Number of backup files that are filled before they are overwritten. The range is 1 to 9 files, with a default of 2 files.
File Size (bytes)	Backup file size. The range is 1 MB to 100 MB with a default of 5 MB.

Configuring a Syslog Policy

When the system boots up, a default syslog policy is created. You can add additional syslog policies or modify existing ones. However, you cannot delete the default syslog policy. For more information on syslog policy attributes, see the Syslog Policy Attributes Table.

The syslog message settings that you configure for the System profile apply to syslog messages only. These settings do not affect other, non- syslog messages.

To add, modify, or delete a syslog policy:

SUMMARY STEPS

1. Choose **Administration > Profile > root > Policies > Syslog**.
2. In the General tab, do one of the following:

DETAILED STEPS

Step 1 Choose **Administration > Profile > root > Policies > Syslog**.

Step 2 In the General tab, do one of the following:

- To add a syslog policy, click **Add Syslog Policy**. Enter the appropriate information and click **OK**
- To edit a syslog policy, select the policy, and then click **Edit**. Edit the appropriate fields and click **OK**.
- To delete a Syslog policy, select the policy, and then click **Delete**.

Syslog Policy Attributes Table

Field	Description
General Tab	
Name	Policy name.
Description	Brief policy description.
Use Emblem Format	Check the check box to use the EMBLEM format for syslog messages. This option appears only on supported devices.
Continue if Host is Down	Check the check box to continue logging if the syslog server is down. This option only appears on supported devices.
Servers Tab	
Add Syslog Server	Click to add a new syslog server.
Syslog Servers table	List of configured syslog servers.
Local Destinations Tab	
Console	• Admin State—Administrative state of the policy: disabled or enabled. • Level—Message level: alert, critical, or emergency. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency.

Field	Description
Monitor	• Admin State—Administrative state of the policy: disabled or enabled. • Level—Message level: emergency, alert, critical, error, warning, notification, information, or debugging. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency.
File	• Admin State—Administrative state of the policy: disabled or enabled. • Level—Message level: emergency, alert, critical, error, warning, notification, information, or debugging. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency. • File Name—Name of the file to which messages are logged. • Size (bytes)—Maximum size, in bytes, that the file can reach before the system begins to overwrite the messages.

Field	Description
Buffer	• Admin State—Administrative state of the policy: disabled or enabled. • Level—Message level: emergency, alert, critical, error, warning, notification, information, or debugging. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency. • Buffer Size (Bytes)—In bytes, the size of the buffer for syslog messages. • Wrap to Flash—Indicates whether or not the buffer contents are saved to flash memory when the buffer wraps (becomes full). Check the check box to save the contents to flash memory if the buffer wraps. • Max File Size in Flash (KB)—Maximum size, in kilobytes, that can be used by the syslog buffer. This option is enabled if the Wrap to Flash option is enabled. • Min Free Flash Size (KB)—Minimum size, in kilobytes, that is allocated for the syslog buffer. This option is enabled if the Wrap to Flash option is enabled.
Time Stamp	Check the check box for each of the following options that you want to enable for timestamp display: • Enable Timestamp • Include Year • Include Milliseconds • Show Time Zone • Use Local Time Zone

Adding a Syslog Server to a Syslog Policy

This procedure assumes that you have already created a syslog policy for a profile. For information on creating a syslog policy for a profile, see Configuring a Syslog Policy, on page 54. For more information on syslog server attributes see the Syslog Server Attributes Table.

SUMMARY STEPS

1. Choose **Administration > Profile > root > Policies > Syslog >** syslog-policy.
2. In the Servers tab, click **Add Syslog Server**. Enter the appropriate information and click **OK**.
3. In the Servers tab, do one of the following:

DETAILED STEPS

Step 1 Choose **Administration > Profile > root > Policies > Syslog >** syslog-policy.

Step 2 In the Servers tab, click **Add Syslog Server**. Enter the appropriate information and click **OK**.

Step 3 In the Servers tab, do one of the following:

- To add a syslog server, click **Add Syslog Server**. Enter the appropriate information and click **OK**
- To edit a syslog server, select the server, and then click **Edit**. Edit the appropriate fields and click **OK**.
- To delete a syslog server, select the server, and then click **Delete**.

Syslog Server Attributes Table

Field	Description
Server Type	One of the following server types: • primary • secondary • tertiary
Hostname/IP Address	Hostname or IP address where the syslog file resides. If you use a hostname, you must configure a DNS server.

Field	Description
Severity	One of the following severity levels: • emergencies (0) • alerts (1) • critical (2) • errors (3) • warnings (4) • notifications (5) • information (6) • debugging (7)
Forwarding Facility	One of the following forwarding facilities: • auth • authpriv • cron • daemon • ftp • kernel • local0 • local1 • local2 • local3 • local4 • local5 • local6 • local7 • lpr • mail • news • syslog • user • uucp
Admin State	Administrative state of the server: disabled or enabled.

Field	Description
Port	Port to use to send data to the syslog server. The default port selection is 514 for UDP.
Protocol	Protocol to use: TCP or UDP (default).
Use Transport Layer Security	Check the check box to use Transport Layer Security. This option is available only for TCP.
Server Interface	Interface to use to access the syslog server.

Modifying the Default Profile

You can add and modify DNS server, NTP server, and policy information associated to the default system profile. However, you cannot create a new DNS domain or delete the default System profile.

SUMMARY STEPS

1. Choose **Administration > Profile > root > Profile > default**.
2. In the General tab, update the information as required:
3. In the Policy tab, update the information as required:
4. Click **Save**.

DETAILED STEPS

Step 1 Choose **Administration > Profile > root > Profile > default**.

Step 2 In the General tab, update the information as required:

Field	Description
Name	Default profile name (read-only).
Description	Brief profile description.
Time Zone	Available time zones. The default time zone is UTC.

Step 3 In the Policy tab, update the information as required:

Field	Description
DNS Servers	
Add DNS Server	Click to add a new DNS server.

Field	Description
Delete	Deletes the DNS server selected in the DNS Servers table.
Up and down arrows	Changes the priority of the selected DNS server. uses the DNS servers in the order in which they appear in the table.
DNS Servers table	Identifies the DNS servers configured in the system.
NTP Servers	
Add NTP Server	Click to add a new NTP server.
Delete	Deletes the NTP server selected in the NTP Servers table.
Up and down arrows	Changes the priority of the selected NTP server. uses the NTP servers in the order in which they appear in the table.
NTP Servers table	Identifies the NTP servers configured in the system.
DNS Domains	
Edit	Edits the DNS domain selected in the DNS Domains table. The default DNS domain cannot be deleted. **Caution** Changing the DNS domain will cause a loss of connectivity that results in an error message, your session closing, and then the display of a new certificate. This situation occurs when the hostname, domain name, or both have changed. If this occurs, reconfigure connectivity with your hypervisor. For more information, see Configuring VM Managers, on page 39.
DNS Domains	Identifies the default DNS domain name and domain configured in the system.
Other Options	
Syslog	The syslog policies associated with this profile can be selected, added, or edited. Click the Resolved Policy field to review or modify the specified policy.
Fault	The fault policies associated with this profile can be selected, added, or edited. Click the Resolved Policy field to review or modify the specified policy.
Core File	The core file policies associated with this profile can be selected, added, or edited. Click the Resolved Policy field to review or modify the specified policy.
Log File	The log file policies associated with this profile can be selected, added, or edited. Click the Resolved Policy field to review or modify the specified policy.

Step 4 Click **Save**.

Editing a DNS Domain

Caution Changing the DNS domain will cause a loss of connectivity that results in an error message, your session closing, and then the display of a new certificate. This situation occurs when the hostname, domain name, or both have changed. If this occurs, reconfigure connectivity with the hypervisor. For more information, see Configuring VM Managers, on page 39.

SUMMARY STEPS

1. Choose **Administration > Profile > root > Profile > default**.
2. Click the **Policy** tab.
3. In the DNS Domains table, select the domain that you want to edit, then click **Edit**.
4. In the Edit DNS Domains dialog box, edit the Domain Name field as required, then click **OK**.
5. Click **Save**.

DETAILED STEPS

Step 1 Choose **Administration > Profile > root > Profile > default**.
Step 2 Click the **Policy** tab.
Step 3 In the DNS Domains table, select the domain that you want to edit, then click **Edit**.
Step 4 In the Edit DNS Domains dialog box, edit the Domain Name field as required, then click **OK**.
Step 5 Click **Save**.

Adding an NTP Server

You can specify a maximum of four NTP servers for the System profile. Use the up and down arrows to arrange the servers from highest to lowest priority, with the highest priority server at the top of the list.

SUMMARY STEPS

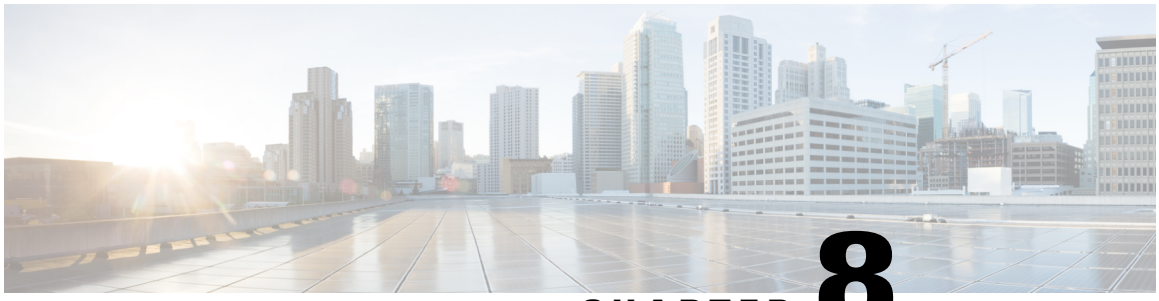
1. Choose **Administration > Profile > root > Profile > default**.
2. In the Policy tab, do one of the following:

DETAILED STEPS

Step 1 Choose **Administration > Profile > root > Profile > default**.

Step 2 In the Policy tab, do one of the following:

- To add an NTP server, click **Add NTP Server**. Enter the appropriate information, click **OK**, and then click **Save**.
- To delete an NTP server, select the server, and then click **Delete**.



CHAPTER 8

Configuring Tenants

This section includes the following topics:

- Tenant Management, page 65
- Configuring Tenants, page 67
- Configuring Virtual Data Centers, page 68
- Configuring Applications, page 70
- Configuring Tiers, page 71

Tenant Management

The topics in this section describe how to manage tenants when is installed in Standalone mode. For information on managing tenants when is installed in Orchestrator mode, see Integrating with DCNM, on page 229.

Tenant Management and Multi-Tenant Environments

provides the ability to support multi-tenant environments. A multi-tenant environment 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 policies, pools, device profiles, service devices, and so on. The administrator can use locales to assign or restrict user privileges and roles by organization if access to certain organizations needs to be restricted.

Users with the tenant-admin role can see only those objects and resources that are related to their associated tenants as defined by the locales and organizations assigned to them. They cannot see the policies or resources of other tenants. Tenant-admin users can view faults only for the resources (such as firewalls or load balancers) that they manage. They cannot see diagnostic information or configure administrative options.

Users with the admin role add a user with the tenant-admin role by associating the user with a locale and organization. For more information about creating user accounts and assigning locales and organizations, see the following topics:

- Creating a User Account, on page 24
- Creating a Locale, on page 21

The tenant-admin role has the following privileges:

- Policy management
- Resource configuration
- Tenant management

provides a strict organizational hierarchy as follows:

1. root
2. Tenant
3. Virtual 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 below the root level are available only to those resources that are below that organization 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-Tenant Environment

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

1. 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, uses that policy or pool.
3. If the policy or pool does not contain available resources at the local level, moves up the hierarchy to the parent organization and checks for a policy with the specified name. repeats this step until the search reaches the root organization.

Note The object name reference resolution takes an object name and resolves an object from an organization container to the object with the same name that is closest in the tree as it searches upward toward root. If an object with the specified name is not found, uses a corresponding default object. For example, assume that there is an SNMP policy under a data center named MySNMP and an SNMP policy in the tenant in the same tree that is also named MySNMP. In this case, the user cannot explicitly select the MySNMP policy under the tenant. If the user wants to select the SNMP policy under the 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, 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 or pool is found, uses it. If a policy is not available, a fault is generated.

Configuring Tenants

Creating a Tenant

SUMMARY STEPS

1. Choose **Tenant Management > root > Create Tenant**.
2. In the Create Tenant dialog box, enter a name and description for the tenant, and then click **OK**.

DETAILED STEPS

Step 1 Choose **Tenant Management > root > Create Tenant**.

Step 2 In the Create Tenant dialog box, enter a name and description for the tenant, and then click **OK**.

Editing a Tenant

SUMMARY STEPS

1. Choose **Tenant Management > root >** *tenant* where *tenant* is the tenant that you want to edit.
2. In the General tab, modify the description as required, and then click **Save**.

DETAILED STEPS

Step 1 Choose **Tenant Management > root >** *tenant* where *tenant* is the tenant that you want to edit.

Step 2 In the General tab, modify the description as required, and then click **Save**.

Deleting a Tenant

Note When you delete an organization (such as a tenant, virtual data center, application, or tier), all data contained under the organization is deleted, including subordinate organizations, service devices, resource pools, and policies.

SUMMARY STEPS

1. Choose **Tenant Management > root**.
2. Right-click the tenant that you want to delete, and choose **Delete Tenant**.
3. When prompted, confirm the deletion.

DETAILED STEPS

Step 1 Choose **Tenant Management > root**.

Step 2 Right-click the tenant that you want to delete, and choose **Delete Tenant**.

Step 3 When prompted, confirm the deletion.

Configuring Virtual Data Centers

Creating a Virtual Data Center

SUMMARY STEPS

1. Choose **Tenant Management > root >** *tenant*, where *tenant* is the location for the new virtual data center.
2. Click **Create Virtual Data Center**.
3. In the Create Virtual Data Center dialog box, enter a name and description for the virtual data center, and then click **OK**.

DETAILED STEPS

Step 1 Choose **Tenant Management > root >** *tenant*, where *tenant* is the location for the new virtual data center.

Step 2 Click **Create Virtual Data Center**.

Step 3 In the Create Virtual Data Center dialog box, enter a name and description for the virtual data center, and then click **OK**.

Editing a Virtual Data Center

SUMMARY STEPS

1. Choose **Tenant Management > root >** *tenant* **>** *vdc* where *vdc* is the virtual data center that you want to edit.
2. In the General tab, modify the description as required and click **Save**.

DETAILED STEPS

Step 1 Choose **Tenant Management > root >** *tenant* **>** *vdc* where *vdc* is the virtual data center that you want to edit.

Step 2 In the General tab, modify the description as required and click **Save**.

Deleting a Virtual Data Center

Note When you delete a virtual data center, all data contained under the virtual data center is deleted, including subordinate organizations, service devices, resource pools, and policies.

SUMMARY STEPS

1. Choose **Tenant Management > root >** *tenant* where *tenant* is the tenant with the virtual data center that you want to delete.
2. Right-click the virtual data center that you want to delete and choose **Delete Virtual Data Center**.
3. When prompted, confirm the deletion.

DETAILED STEPS

Step 1 Choose **Tenant Management > root >** *tenant* where *tenant* is the tenant with the virtual data center that you want to delete.

Step 2 Right-click the virtual data center that you want to delete and choose **Delete Virtual Data Center**.

Step 3 When prompted, confirm the deletion.

Configuring Applications

Creating an Application

SUMMARY STEPS

1. Choose **Tenant Management > root >** *tenant* **>** *vdc* where *vdc* is the location for the new application.
2. Click **Create Application**.
3. In the Create Application dialog box, enter a name and description for the application, and then click **OK**.

DETAILED STEPS

Step 1 Choose **Tenant Management > root >** *tenant* **>** *vdc* where *vdc* is the location for the new application.

Step 2 Click **Create Application**.

Step 3 In the Create Application dialog box, enter a name and description for the application, and then click **OK**.

Editing an Application

SUMMARY STEPS

1. Choose **Tenant Management > root >** *tenant* **>** *vdc* **>** *application*, where *application* is the application that you want to edit.
2. In the General tab, modify the description as required, and then click **Save**.

DETAILED STEPS

Step 1 Choose **Tenant Management > root >** *tenant* **>** *vdc* **>** *application*, where *application* is the application that you want to edit.

Step 2 In the General tab, modify the description as required, and then click **Save**.

Deleting an Application

Note When you delete an application, all data contained under the application is deleted, including subordinate organizations, service devices, resource pools, and policies.

SUMMARY STEPS

1. Choose **Tenant Management > root >** *tenant* **>** *vdc* where *vdc* is the virtual data center with the application that you want to delete.
2. Right-click the application that you want to delete, and choose **Delete Application**.
3. When prompted, confirm the deletion.

DETAILED STEPS

Step 1 Choose **Tenant Management > root >** *tenant* **>** *vdc* where *vdc* is the virtual data center with the application that you want to delete.

Step 2 Right-click the application that you want to delete, and choose **Delete Application**.

Step 3 When prompted, confirm the deletion.

Configuring Tiers

Creating a Tier

SUMMARY STEPS

1. Choose **Tenant Management > root >** *tenant* **>** *vdc* **>** *application*, where *application* is the location for the new tier.
2. Click **Create Tier**.
3. In the Create Tier dialog box, enter a name and description for the tier, and then click **OK**

DETAILED STEPS

Step 1 Choose **Tenant Management > root >** *tenant* **>** *vdc* **>** *application*, where *application* is the location for the new tier.
Step 2 Click **Create Tier**.
Step 3 In the Create Tier dialog box, enter a name and description for the tier, and then click **OK**

Editing a Tier

SUMMARY STEPS

1. Choose **Tenant Management > root >** *tenant* **>** *vdc* **>** *application* **>** *tier* where *tier* is the tier you want to edit.
2. In the General tab, modify the description as required, and then click **Save**.

DETAILED STEPS

Step 1 Choose **Tenant Management > root >** *tenant* **>** *vdc* **>** *application* **>** *tier* where *tier* is the tier you want to edit.
Step 2 In the General tab, modify the description as required, and then click **Save**.

Deleting a Tier

Note When you delete a tier, all data contained under it is also deleted, including service devices, resource pools, and policies.

SUMMARY STEPS

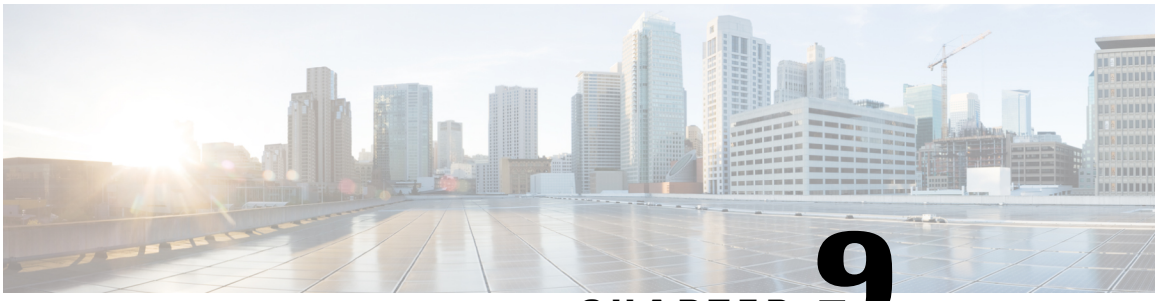
1. Choose **Tenant Management > root >** *tenant* **>** *vdc* **>** *application* where *application* contains the tier that you want to delete.
2. Right-click the tier that you want to delete and choose **Delete Tier**.
3. When prompted, confirm the deletion.

DETAILED STEPS

Step 1 Choose **Tenant Management > root >** *tenant* **>** *vdc* **>** *application* where *application* contains the tier that you want to delete.

Step 2 Right-click the tier that you want to delete and choose **Delete Tier**.

Step 3 When prompted, confirm the deletion.



CHAPTER 9

Configuring Service Policies and Profiles

This section includes the following topics:

- Service Path Configuration Workflow, page 75
- Configuring Service Policies, page 81
- Working with Profiles, page 120
- Configuring Security Profiles, page 128
- Configuring Security Policy Attributes, page 133

Service Path Configuration Workflow

Service paths enable you to apply multiple services to VM traffic by binding a sequence of services to a specific port profile.

The following table identifies the tasks required to configure a service path, related topics, and the minimum role required for each task:

Task	Related Topic	Role Required
1. Confirm that the prerequisites are met.	See Prerequisites for Configuring Service Paths, on page 76.	admin
2. Create the tenant and, if needed, the subordinate organization in which the service path will reside.	See Creating a Tenant, on page 67.	admin
3. Add a port profile to a Nexus 1000V VSM. **Note** You can perform this step at any time before Step 6.	See Adding a Port Profile to a VSM, on page 77.	admin
4. Create service nodes for inclusion in the service path.	See Creating a Service Node, on page 78.	tenant-admin

Task	Related Topic	Role Required
5. Create a service path with service entries.	See Creating a Service Path, on page 79.	tenant-admin
6. Bind the service path to the VSM port profile.	See Binding a Service Path to a Port Profile, on page 80.	tenant-admin

Prerequisites for Configuring Service Paths

The following table describes the prerequisites for configuring service paths:

Item	Requirement
Tenant	Has at least one of the following assigned: • Compute firewall • Edge firewall • vPath-enabled load balancer using Citrix NetScaler 1000V
Compute firewall	• Has a security policy assigned. • Has a policy set with policies and rules for the compute firewall. • The policy set is bound to the compute firewall security policy. • A VLAN is provided if the firewall is to be used as a Layer 2 adjacent service node. • The VLAN exists on the VSM.
Edge firewall	• Has an edge device profile defined. • Has an edge security profile defined. • Has a policy set with policies and rules for the edge firewall. • An inbound security profile is attached to the outside interface of the edge firewall. • A VLAN is provided on the data interface because the edge firewall can be used only as a Layer 2 adjacent service node. • The VLAN exists on the VSM.
Load Balancer	Has vPath enabled.

Item	Requirement
Nexus 1000V	• Is deployed. • Is registered with Prime Network Services Controller.
Services	The following services are deployed: • VSG • ASA 1000V • Citrix NetScaler 1000V

Adding a Port Profile to a VSM

enables you to add a port profile to an enterprise VSM. You cannot add a port profile to a cloud VSM.

If an enterprise VSM has preconfigured port profiles or virtual service configurations that were created outside of , these configurations will not be displayed in the GUI.

If you create a port profile in and specify a VLAN, you must create the VLAN itself on the VSM and then add it to the necessary system and uplink port profiles. The same steps apply for VLANs that you specify while creating service devices, such as edge or compute firewalls: you must create the VLANs on the devices, and then add them to the appropriate system and uplink port profiles.

Before You Begin

Confirm the following:

- An enterprise VSM is registered and in the *applied* state in by choosing **Resource Management > Resources > VSMs**.
- You have admin privileges.

SUMMARY STEPS

1. Choose **Resource Management > Resources > VSMs >** *vsm*, then click **Edit**.
2. Above the Port Profile table, click **Add**.
3. In the Add Port Profile dialog box, enter the required information as follows, then click **OK**:

DETAILED STEPS

Step 1 Choose **Resource Management > Resources > VSMs >** *vsm*, then click **Edit**.

Step 2 Above the Port Profile table, click **Add**.

Step 3 In the Add Port Profile dialog box, enter the required information as follows, then click **OK**:

1 In the General tab, provide the following information:

- Name
- Description
- State: Enabled or Disabled.
- Type of Binding: Dynamic, Ephemeral, or Static.
- Binding Option: Auto, AutoExpand, or None.
- Maximum and minimum number of ports.
- Tenant or subordinate organization in which to create the port profile.

2 In the L2 Network Membership tab, provide the following information:

- Capability: Bridge Domain or VLAN.
- Mode: Access or Trunk
- VLAN number (Access mode) or VLAN range (Trunk mode).

The NICs table is populated automatically after you bind a service path to the port profile and the service path is used the first time. For more information about configuring a service path and binding it to a port profile, see Service Path Configuration Workflow, on page 75.

Creating a Service Node

A service node identifies a virtual service device that can be used in a service path and provides basic configuration for that device.

The following restrictions apply when creating a service node:

- If you create multiple service nodes for a specific logical service device, the adjacencies must be different.
- You cannot create service nodes under different tenants with the same data IP address, VLAN, and adjacency, even if the logical service devices are different.

If either of these situations occurs, an error message will be generated when you attempt to bind the service path to the VSM port profile.

Before You Begin

Confirm the following:

- A logical device (compute firewall, edge firewall, or load balancer) exists.
- You have Tenant Management privileges.

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root >** *tenant* **> Policy Helpers > Service Node**, and then click **Add Service Node**.
2. In the Add Service Node dialog box, provide the following information, and then click **OK**:

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root >** *tenant* **> Policy Helpers > Service Node**, and then click **Add Service Node**.

Step 2 In the Add Service Node dialog box, provide the following information, and then click **OK**:

- Name
- Service Type: Compute Firewall, Edge Firewall, or Load Balancer.
- Network Service: Name of the logical service device.
- Fail Mode: Action to take if the service node loses connectivity:
  - Close—Drop the packets.
  - Open—Forward the packets.
- Adjacency Type: Layer 2 or Layer 3.

Creating a Service Path

After you create service nodes, you can create a service path that uses the nodes. Traffic using the service path moves from one service node to another in the sequence that you specify.

Note You cannot use a service node more than once in a service path.

Before You Begin

Confirm that you have Tenant Management privileges.

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root >** *tenant* **> Policies > Service Path**, and then click **Add Service Path**.
2. In the Add Service Path dialog box, enter a name and description for the service path, and then click **Add Service Entry**.
3. In the Add Service Entry dialog box, provide the following information, and then click **OK**:
4. Add additional service entries as needed for the service path and click **OK**.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root >** *tenant* **> Policies > Service Path**, and then click **Add Service Path**.

Step 2 In the Add Service Path dialog box, enter a name and description for the service path, and then click **Add Service Entry**.

Step 3 In the Add Service Entry dialog box, provide the following information, and then click **OK**:

- Service type
- Service node
- Service profile

The service profile identifies the policies that apply to the traffic using the service path.

Step 4 Add additional service entries as needed for the service path and click **OK**.

What to Do Next

You must bind the service path to a port profile so that the service path can be created on the Nexus 1000V VSM. After the service path is bound to a port profile, the traffic using that port profile follows the service entries in the sequence indicated in the table.

Binding a Service Path to a Port Profile

Binding a service path to a port profile ensures that all traffic using that port profile will follow the configured service path. When you bind a service path to a port profile, the NICs table that is displayed in the Edit Port Profile dialog box remains empty until the service path is used for the first time. When the service path is used, the NICs table is populated automatically.

Before You Begin

Confirm the following:

- A service path exists.
- You have Tenant Management privileges.

Step 1 Choose one of the following:

- **Resource Management > Managed Resources > root >** *tenant* **> Port Profiles Tab**
- **Resource Management > Resources > VSMs >** *vsm* **> Edit**

Step 2 In the Port Profiles table, select the port profile you want to bind a service path to, then click **Edit**.

Step 3 In the Service Path field, click **Select**.

Step 4 In the Select Service Path dialog box, select the required service path, then click **OK**.

Step 5 In the Edit Port Profile dialog Box, click **Apply** and then **OK** to apply and save the change.

Configuring Service Policies

This procedure describes the general steps for configuring service policies for managed resources.

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policies > *policy-type***.
2. In the General tab, click **Add *policy-type***.
3. In the dialog boxes that follow, enter the required information. For more information on each dialog box, click the online-help.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policies > *policy-type***.

Step 2 In the General tab, click **Add *policy-type***.

Step 3 In the dialog boxes that follow, enter the required information. For more information on each dialog box, click the online-help.
The following topics provide specific details on various policies:

- Configuring ACL Policies and Policy Sets, on page 82
- Configuring Connection Timeout Policies, on page 88
- Configuring DHCP Policies, on page 90
- Configuring IP Audit and IP Audit Signature Policies, on page 93
- Configuring NAT/PAT Policies and Policy Sets, on page 96
- Configuring Packet Inspection Policies, on page 101
- Configuring Routing Policies, on page 103
- Configuring TCP Intercept Policies, on page 103
- Configuring Site-to-Site IPsec VPN Policies, on page 105

Configuring ACL Policies and Policy Sets

The following topics describe how to configure ACL policies and policy sets:

- Adding an ACL Policy, on page 82
- Time Ranges in ACL Policy Rules, on page 86
- Adding an ACL Policy Set, on page 87

Adding an ACL Policy

enables you to implement access control lists based on the time of day and frequency, or inclusion in a defined group. Benefits of this feature include:

- Providing closer control of access to network resources throughout the day or week.
- Enhancing policy-based routing and queuing functions.
- Automatically rerouting traffic at specific times of the day to ensure cost-effectiveness.

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policies > ACL > ACL Policies**.
2. In the General tab, click **Add ACL Policy**.
3. In the Add ACL Policy dialog box, enter a name and brief description for the policy, then click **Add Rule**.
4. In the Add Rule dialog box, specify the required information as described in Add ACL Policy Rule Dialog Box, on page 83, then click **OK**.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policies > ACL > ACL Policies**.

Step 2 In the General tab, click **Add ACL Policy**.

Step 3 In the Add ACL Policy dialog box, enter a name and brief description for the policy, then click **Add Rule**.

Step 4 In the Add Rule dialog box, specify the required information as described in Add ACL Policy Rule Dialog Box, on page 83, then click **OK**.

Note All Network Port conditions in a single ACL rule must have the same value selected in the Attribute Value field. For example, you would choose FTP from the Attribute Value drop-down list for all rule conditions that specify the Attribute Name of Network Port.

The Add Rule dialog box contains settings for time rules for ACL policies. For more information about using time ranges with ACL policies, see Time Ranges in ACL Policy Rules, on page 86.

Add ACL Policy Rule Dialog Box

Field	Description
Name	Rule name, containing 2 to 32 characters. The name can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:). You cannot change the name after it is saved.
Description	Brief rule description, containing 1 to 256 characters. The name can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:).
Action to Take	1 Click the action to take if the rule conditions are met: • **Drop—**Drops traffic or denies access. • **Permit—**Forwards traffic or allows access. • **Reset—**Resets the connection. 2 Check the **Log** check box to enable logging.
Condition Match Criteria	Do one of the following: • Click **match-all** for the ACL Policy Rule to match all the conditions (AND). • Click **match-any** for the ACL Policy Rule to match any one condition (OR).
Src-Dest-Service Tab A rule can have a service condition or a protocol condition, but not both.	
Source Conditions	1 Click **Add**. 2 Enter the required values for following: • Attribute Type • Attribute Name • Operator • Attribute Value 3 Click **OK**.

Field	Description
Destination Conditions	**1** Click **Add**. **2** Enter the required values for following: • Attribute Type • Attribute Name • Operator • Attribute Value **3** Click **OK**.
Service	**1** Click **Add**. **2** Enter the required values for following: • Operator • Protocol • Port **3** Click **OK**.
Protocol Tab	Specify the protocols to which the rule applies: • To apply the rule to any protocol, check the **Any** check box. • To apply the rule to specific protocols: **1** Uncheck the **Any** check box. **2** From the **Operator** drop-down list, choose a qualifier: Equal, Not Equal, Member, Not Member, In range, or Not in range. **3** In the Value fields, specify the protocol, object group, or range.
Ether Type Tab	Specify the encapsulated protocols to be examined for this rule: **1** From the Operator drop-down list, choose a qualifier: Equal, Not equal, Greater than, Less than, Member, Not Member, In range, or Not in range. **2** In the Value fields, specify the hexadecimal value, object group, or hexadecimal range.
Time Range Tab	
To apply the rule all the time	Check the **Always** check box.

Field	Description
To apply the rule for a specific time range	**1** Uncheck the **Always** check box. **2** Check the **Range** check box. **3** In the Absolute Start Time fields, provide the start date and time. **4** In the Absolute End Time fields, provide the end date and time.
To apply the rule based on membership in an object group	**1** Uncheck the **Always** check box. **2** Check the **Pattern** check box. **3** From the Operator drop-down list, choose **member (Member of)**. **4** Do any of the following : • From the **Select Object Group** drop-down list, choose an existing object group. • Click **Add Object Group** to create a new object group. • Click the Resolved Object Group link to review or modify the specified object group.
To apply the rule on a periodic basis, with the frequency you specify	**1** Uncheck the **Always** check box. **2** Check the **Pattern** check box. **3** From the Operator drop-down list, choose **range (In range)**. **4** In the Begin fields: **a** From the Begin drop-down list, choose the beginning day of the week or the frequency of the time range. **b** Choose the beginning hour and minute, and AM or PM. **5** In the End fields: **a** From the End drop-down list, choose the ending day of the week or frequency. **b** Choose the ending hour and minute, and AM or PM. **Note** If you choose a frequency from the Begin drop-down list, choose the same frequency from the End drop-down list. For example, choose Weekdays from both the Begin and End drop-down lists.

Field	Description
Advanced Tab	Specify any source port attributes that must be matched for the current policy to apply: **1** Click **Add**. **2** Provide the required information in the following fields, and then click **OK**: • Attribute Name • Operator • Attribute Value

Time Ranges in ACL Policy Rules

enables you to configure time ranges for ACL policy rules in either of the following ways:

- By specifying a time range for the ACL policy rule.
- By associating an ACL object group with the ACL policy rule.

supports the following types of time ranges:

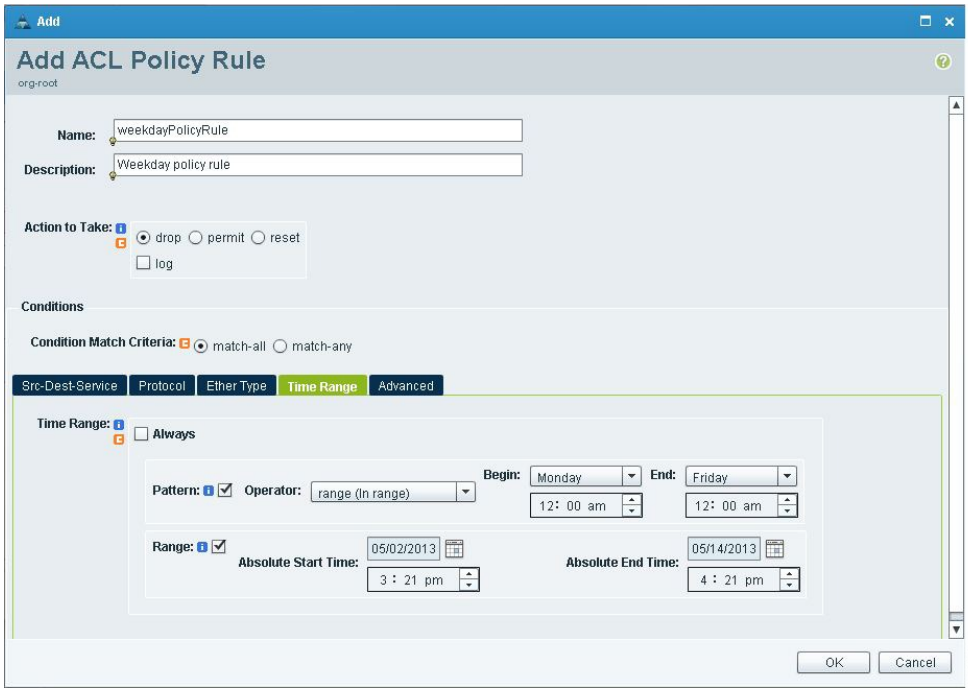
- Periodic—Specified by day-of-week start and end times (such as Sunday to Sunday), or a frequency (such as Daily, Weekdays, or Weekends). Periodic range start and end times also include options for hours and minutes.
- Absolute—Specified by a calendar date and time for start and end times, such as 01 Sep 2013 12:00 AM to 31 Dec 2013 12:00 AM.

For each ACL policy rule, you can have:

- One absolute time range.
- Any number of periodic time ranges, or none.
    - To specify a single periodic time range, add it to an ACL policy rule.
    - To specify multiple periodic time ranges, use an ACL policy object group.

The following figure shows the Time Range fields for an ACL policy rule.

Figure 2: Time Range Fields in an ACL Policy Rule



Adding an ACL Policy Set

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policies > ACL > ACL Policy Sets**.
2. In the General tab, click **Add ACL Policy Set**.
3. In the Add ACL Policy Set dialog box, enter the required information as described in the following table, then click **OK**:

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policies > ACL > ACL Policy Sets**.

Step 2 In the General tab, click **Add ACL Policy Set**.

Step 3 In the Add ACL Policy Set dialog box, enter the required information as described in the following table, then click **OK**:

Field	Description
Name	Policy set name, containing 2 to 32 characters. The name can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:). You cannot change the name after it is saved.

Field	Description
Description	Policy set description, containing 1 to 256 characters. The name can contain alphanumeric characters, hyphen (-), underscore (_), period (.), and colon (:).
Admin State	Administrative state of the policy: enabled or disabled. This field is not available for all policy sets.
Policies	
Add Policy	Click to add a new policy.
Available	Policies that can be assigned to the policy set. Use the arrows between the columns to move policies between columns.
Assigned	Policies assigned to the policy set.
Up and down arrows	Changes the priority of the selected policies. Arrange the policies from highest to lowest priority, with the highest priority policy at the top of the list.

Configuring Connection Timeout Policies

enables you to configure connection timeout policies so that you can establish timeout limits for different traffic types.

After you create a connection timeout policy, you can associate it with an edge security profile. For more information, see Configuring Edge Security Profiles, on page 124.

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policies > Connection Timeout**.
2. In the General tab, click **Add Connection Timeout Policy**.
3. In the Add Connection Timeout Policy dialog box:
4. To add a rule to the policy, click **Add Rule**.
5. In the Add Connection Timeout Policy Rule dialog box, provide the information as described in Add Connection Timeout Policy Rule Dialog Box, on page 89.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policies > Connection Timeout**.

Step 2 In the General tab, click **Add Connection Timeout Policy**.

Step 3 In the Add Connection Timeout Policy dialog box:

a) Enter a policy name and description.

b) Choose whether the administrative status of the policy is to be enabled or disabled.

Step 4 To add a rule to the policy, click **Add Rule**.

Step 5 In the Add Connection Timeout Policy Rule dialog box, provide the information as described in Add Connection Timeout Policy Rule Dialog Box, on page 89.

Add Connection Timeout Policy Rule Dialog Box

Field	Description
Name	Policy name.
Description	Brief policy description.
Action	
Idle TCP	Length of time (in days, hours, minutes, and seconds) a TCP connection can remain idle before it is closed.
Half-Closed	Length of time (in days, hours, minutes, and seconds) a half-closed TCP connection can remain idle before it is freed.
Send Reset To Idle Connection	Check the check box to send a reset to the TCP endpoints when a TCP connection times out.
Idle UDP	Length of time (in days, hours, minutes, and seconds) a UDP connection can remain idle before it closes. The duration must be at least one minute, and the default value is two minutes. Enter 00:00:00:00 to disable timeout.
ICMP	Length of time (in days, hours, minutes, and seconds) an ICMP state can remain idle before it is closed.
Protocol	Not available for configuration.
Source Conditions	
Destination Conditions	

Configuring DHCP Policies

enables you to create the following DHCP policies and apply them to edge firewalls:

- DHCP relay policy
- DHCP server policy

You can also configure DHCP relay servers for inclusion in DHCP relay policies.

The DHCP relay and DHCP server policies can be authored at the organization level and can be applied only to the inside interface of an edge firewall. When they are applied, DHCP policies allow the edge firewall to act either as a DHCP server or a DHCP relay for all VMs in the inside network.

You can apply only one DHCP server or relay profile at a time to the inside interface of the edge firewall.

For more information, see the following topics:

- Adding a DHCP Relay Server, on page 90
- Configuring a DHCP Relay Policy, on page 91
- Configuring a DHCP Server Policy, on page 92

Adding a DHCP Relay Server

DHCP relay servers are used to forward DHCP requests and replies between clients and servers when they are not on the same physical subnet. In contrast to IP router forwarding, where IP datagrams are switched between networks, DHCP relay servers receive DHCP messages and then generate a new message to send out on a different interface.

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policies > DHCP > DHCP Relay Server**.
2. In the General tab, click **Add DHCP Relay Server**.
3. In the New DHCP Relay Server dialog box, provide the information described in the Add DHCP Relay Server Dialog Box, on page 91, then click **OK**.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policies > DHCP > DHCP Relay Server**.

Step 2 In the General tab, click **Add DHCP Relay Server**.

Step 3 In the New DHCP Relay Server dialog box, provide the information described in the Add DHCP Relay Server Dialog Box, on page 91, then click **OK**.

Add DHCP Relay Server Dialog Box

Field	Description
Name	Relay server name.
Description	Brief description of the relay server.
Relay Server IP	IP address of the relay server.
Interface Name	Interface to use to reach the relay server.

Configuring a DHCP Relay Policy

enables you to associate a DHCP relay server with a DHCP relay policy, as described in this procedure.

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policies > DHCP > DHCP Relay**.
2. In the General tab, click **Add DHCP Relay Policy**.
3. In the New DHCP Relay Policy dialog box, provide the information described in Add DHCP Relay Policy Dialog Box, on page 91, then click **OK**.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policies > DHCP > DHCP Relay**.

Step 2 In the General tab, click **Add DHCP Relay Policy**.

Step 3 In the New DHCP Relay Policy dialog box, provide the information described in Add DHCP Relay Policy Dialog Box, on page 91, then click **OK**.

Add DHCP Relay Policy Dialog Box

Name	Description
Name	Policy name.
Description	Brief policy description.

Name	Description
DHCP Relay Server Assignment	Assign a DHCP relay server in one of the following ways: • Click **Add DHCP Relay Server** to add a new DHCP relay server. • In the Available Relay Servers list, select one of the available relay servers and move it to the Assigned Relay Servers list. You must assign at least one DHCP relay server to the policy.

Configuring a DHCP Server Policy

A DHCP server policy enables you to define the characteristics of the policy, such as ping and lease timeouts, IP address range, and DNS and WINS settings.

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policies > DHCP > DHCP Server**.
2. In the General tab, click **Add DHCP Server Policy**.
3. In the New DHCP Server Policy dialog box, provide the information as described in Add DHCP Server Policy Dialog Box, on page 92, then click **OK**.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policies > DHCP > DHCP Server**.

Step 2 In the General tab, click **Add DHCP Server Policy**.

Step 3 In the New DHCP Server Policy dialog box, provide the information as described in Add DHCP Server Policy Dialog Box, on page 92, then click **OK**.

Add DHCP Server Policy Dialog Box

Field	Description
General Tab	
Name	Policy name.
Description	Brief policy description.
Ping Timeout (Milliseconds)	Amount of time (in milliseconds) that the DHCP server waits for a ping reply before it stops attempting to reach a pool address for client assignment. The valid range is 10 to 10000 milliseconds.

Field	Description
Lease Timeout	Amount of time (in days, hour, minutes, and seconds) that the DHCP server allocates an IP address to a DHCP client before reclaiming and then reallocating it to another client. The default value is 00:01:00:00 (one hour).
Edge Device Interface Using the DHCP Client for DHCP Server Auto Configuration	To enable DHCP server automatic configuration, enter the name of the edge device interface that uses the DHCP client. For ASA 1000V instances, this interface is always an outside interface. Leaving this field empty indicates that the automatic configuration feature is disabled.
DNS Settings	DNS settings used by the edge firewall when configuring DHCP clients. To add a new entry, click **Add DNS Setting** and add the required information.
WINS Servers	Windows Internet Naming Service (WINS) name servers that are available to DHCP clients. To add a new WINS server, click **Add WINS Server** and enter the WINS server IP address. WINS servers are listed in the order of preference, with the most preferred WINS server at the top. Select an entry in the table, and then use the arrows above the table to change server priority.
IP Address Range	Enter the following information for the DHCP address pool: • Start IP Address—Beginning IP address of the pool. • End IP Address—Ending IP address of the pool. • Subnet Mask—Subnet mask to apply to the address pool.

The Advance tab allows you to add Manual and Exclude addresses. You must know the applicable MAC and IP addresses.

Configuring IP Audit and IP Audit Signature Policies

The IP audit feature provides basic Intrusion Prevention System (IPS) support for ASA 1000V instances. supports a basic list of signatures, and enables you to configure policies that specify one or more actions to apply to traffic that matches a signature.

The following IP audit policies are available:

- Audit policies
- Signature policies

When you associate an IP audit policy with a device, the policy is applied to all traffic on the outside interface of the device.

The following topics describe how to configure these policies.

Configuring IP Audit Policies

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policies > IP Audit > Audit Policies**.
2. In the General tab, click **Add IP Audit Policy**.
3. In the Add IP Audit Policy dialog box provide the following information:
   - Policy name
   - Policy description
   - In the Admin State field, choose whether the administrative state of the policy is to be enabled or disabled.
4. To add a rule to the policy, click **Add Rule** in the Rule Table toolbar.
5. In the Add IP Audit Policy Rule dialog box, provide the information as described in Add IP Audit Policy Rule Dialog Box, on page 94, then click **OK** in the open dialog boxes.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policies > IP Audit > Audit Policies**.

Step 2 In the General tab, click **Add IP Audit Policy**.

Step 3 In the Add IP Audit Policy dialog box provide the following information:

- Policy name
- Policy description
- In the Admin State field, choose whether the administrative state of the policy is to be enabled or disabled.

Step 4 To add a rule to the policy, click **Add Rule** in the Rule Table toolbar.

Step 5 In the Add IP Audit Policy Rule dialog box, provide the information as described in Add IP Audit Policy Rule Dialog Box, on page 94, then click **OK** in the open dialog boxes.

Add IP Audit Policy Rule Dialog Box

Field	Description
Name	Rule name.
Description	Brief rule description.

Field	Description
Attack-Class Action	Check the check boxes of the actions to take for signature type Attack if the conditions of the rule are met: • Log—Send a message indicating that a packet matched the signature. • Drop—Drop the packet. • Reset Flow—Drop the packet and reset the connection.
Informational-Class Action	Check the check boxes of the actions to take for signature type Informational if the conditions of the rule are met: • Log—Send a message indicating that a packet matched the signature. • Drop—Drop the packet. • Reset Flow—Drop the packet and reset the connection.
Protocol	Not available for configuration.
Source Conditions	
Destination Conditions	

Configuring IP Audit Signature Policies

An IP audit signature policy identifies the signatures that are enabled and disabled. By default, all signatures are enabled. You can disable a signature when legitimate traffic matches the signature in most situations, resulting in false alarms. However, disabling the signature is performed at a global level, meaning that no traffic will trigger the signature (even bad traffic) when it is disabled.

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policies > IP Audit > Signature Policies**.
2. In the General tab, click **Add IP Audit Signature Policy**.
3. In the Add IP Audit Signature Policy dialog box, enter a name and description for the policy.
4. In the Signatures area, move signatures between the Enabled Signatures and Disabled Signatures lists as required.
5. After you have made all adjustments, click **OK**.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policies > IP Audit > Signature Policies**.

Step 2 In the General tab, click **Add IP Audit Signature Policy**.

Step 3 In the Add IP Audit Signature Policy dialog box, enter a name and description for the policy.

Step 4 In the Signatures area, move signatures between the Enabled Signatures and Disabled Signatures lists as required.

Note We recommend that you do not disable signatures unless you are sure you understand the consequences of doing so.

You can view additional information about a signature by selecting the required signature and clicking **Properties**.

Step 5 After you have made all adjustments, click **OK**.

Configuring NAT/PAT Policies and Policy Sets

supports Network Address Translation (NAT) and Port Address Translation (PAT) policies for controlling address translation in the deployed network. These policies support both static and dynamic translation of IP addresses and ports.

enables you to configure the following policy items:

- NAT policy—Can contain multiple rules, which are evaluated sequentially until a match is found.

Note Edge routers support a limited set of NAT policy options.

- NAT policy set—Group of NAT policies that can be associated with an edge security profile. When the profile is applied, the NAT policies are applied only to ingress traffic.
- PAT policy—Supports source dynamic and destination static interface PAT on edge firewalls.

The following topics describe how to configure NAT and PAT policies, and NAT policy sets.

Configuring NAT/PAT Policies

This procedure describes how to configure NAT/PAT policies with .

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policies > NAT > NAT Policies**.
2. In the General tab, click **Add NAT Policy**.
3. In the Add NAT Policy dialog box, enter a name and description for the policy.
4. In the Admin State field, indicate whether the administrative state of the policy is to be enabled or disabled.
5. To add a rule to the policy, click **Add Rule**.
6. In the Add NAT Policy Rule dialog box, provide the information as described in Add NAT Policy Rule Dialog Box, on page 97, then click **OK** in the open dialog boxes.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policies > NAT > NAT Policies**.

Step 2 In the General tab, click **Add NAT Policy**.

Step 3 In the Add NAT Policy dialog box, enter a name and description for the policy.

Step 4 In the Admin State field, indicate whether the administrative state of the policy is to be enabled or disabled.

Step 5 To add a rule to the policy, click **Add Rule**.

Step 6 In the Add NAT Policy Rule dialog box, provide the information as described in Add NAT Policy Rule Dialog Box, on page 97, then click **OK** in the open dialog boxes.

Add NAT Policy Rule Dialog Box

Add NAT Policy Rule Dialog Box

Field	Description
Name	Rule name.
Description	Brief rule description.
Original Packet Match Conditions	
Source Match Conditions	Source attributes that must be matched for the current policy to apply. To add a new condition, click **Add Rule Condition**. Available source attributes are IP Address and Network Port.
Destination Match Conditions	Destination attributes that must be matched for the current policy to apply. To add a new condition, click **Add Rule Condition**. Available destination attributes are IP Address and Network Port.
Protocol	Specify the protocols to which the rule applies: • To apply the rule to any protocol, check the **Any** check box. • To apply the rule to specific protocols: **1** Uncheck the **Any** check box. **2** From the Operator drop-down list, choose a qualifier: Equal, Not equal, Member, Not Member, In range, or Not in range. **3** In the Value fields, specify the protocol, object group, or range.
NAT Action Table	

Field	Description
NAT Action	From the drop-down list, choose the required translation option: Static or Dynamic.
Translated Address	Identify a translated address pool for each original packet match condition from the following options: • Source IP Pool • Source Port Pool • Source IP PAT Pool • Destination IP Pool • Destination Port Pool For example, if you specify a source IP address match condition, you must identify a Source IP Pool object group. Similarly, a destination network port match requires a Destination Port Pool object group. The Source IP PAT Pool option is available only if you choose dynamic translation. Click **Add Object Group** to add object groups for the translation actions.
NAT Options	Check and uncheck the check boxes as required: • Enable Bidirectional—Check the check box for connections to be initiated bidirectionally; that is, both to and from the host. Available only for static address translation. • Enable DNS—Check the check box to enable DNS for NAT. • Enable Round Robin IP—Check the check box to allocate IP addresses on a round-robin basis. Available only for dynamic address translation. • Disable Proxy ARP—Check the check box to disable proxy ARP. Available only for static address translation.

Note Edge routers support a limited set of NAT policy options.

Configuring NAT Policy Sets

Policy sets enable you to group multiple policies of the same type (such as NAT, ACL, or Interface) for inclusion in a profile. NAT policy sets are groups of NAT policies that can be associated with an edge security profile.

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policies > NAT > NAT Policy Sets**.
2. In the General tab, click **Add NAT Policy Set**.
3. In the Add NAT Policy Set dialog box, enter a name and description for the policy set.
4. In the Admin State field, indicate whether the administrative status of the policy is to be enabled or disabled.
5. In the Policies area, select the policies to include in this policy set:
6. Click **OK**.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policies > NAT > NAT Policy Sets**.

Step 2 In the General tab, click **Add NAT Policy Set**.

Step 3 In the Add NAT Policy Set dialog box, enter a name and description for the policy set.

Step 4 In the Admin State field, indicate whether the administrative status of the policy is to be enabled or disabled.

Step 5 In the Policies area, select the policies to include in this policy set:

a) In the Available list, select one or more policies and move them to the Assigned list.
b) Adjust the priority of the assigned policies by using the arrow keys above the list.
c) If required, click **Add NAT Policy** to add a new policy and include it in the Assigned list.
For information on configuring a NAT policy, see Configuring NAT/PAT Policies, on page 96.

Step 6 Click **OK**.

Configuring PAT for Edge Firewalls

enables you to configure source and destination interface PAT for edge firewalls, such as the ASA 1000V. For more information, see the following topics.

Configuring Source Dynamic Interface PAT

enables you to configure source dynamic interface PAT for edge firewalls, such as ASA 1000Vs.

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policies > NAT > NAT Policies**.
2. In the General tab, click **Add NAT Policy**.
3. In the Add NAT Policy dialog box, enter a name and description for the policy.
4. In the Admin State field, indicate whether the administrative state of the policy is to be enabled or disabled.
5. Click **Add Rule** to add a rule to this policy.
6. In the Add NAT Policy Rule dialog box, provide the information described in Add NAT Policy Rule Dialog Box, on page 97 with the following specific settings, then click **OK**:
7. Click **OK**.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policies > NAT > NAT Policies**.

Step 2 In the General tab, click **Add NAT Policy**.

Step 3 In the Add NAT Policy dialog box, enter a name and description for the policy.

Step 4 In the Admin State field, indicate whether the administrative state of the policy is to be enabled or disabled.

Step 5 Click **Add Rule** to add a rule to this policy.

Step 6 In the Add NAT Policy Rule dialog box, provide the information described in Add NAT Policy Rule Dialog Box, on page 97 with the following specific settings, then click **OK**:

a) From the NAT Action drop-down list, choose **Dynamic**.

b) In the Translated Address area, add a Source IP Pool object group that contains the ASA 1000V outside interface IP address.

Step 7 Click **OK**.

Configuring Destination Static Interface PAT

enables you to configure destination static interface PAT for edge firewalls, such as ASA 1000Vs, as described in the following procedure.

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policies > NAT > NAT Policies**.
2. In the General tab, click **Add NAT Policy**.
3. In the Add NAT Policy dialog box, enter a name and description for the policy.
4. In the Admin State field, indicate whether the administrative state of the policy is to be enabled or disabled.
5. Click **Add Rule** to add a rule to this policy.
6. In the Add NAT Policy Rule dialog box, enter the IP address of the ASA 1000V outside interface as a rule condition for Destination Match Conditions.
7. Configure other options in the Add NAT Policy Rule dialog box as described in Add NAT Policy Rule Dialog Box, on page 97, then click **OK**.
8. Click **OK**.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policies > NAT > NAT Policies**.

Step 2 In the General tab, click **Add NAT Policy**.

Step 3 In the Add NAT Policy dialog box, enter a name and description for the policy.

Step 4 In the Admin State field, indicate whether the administrative state of the policy is to be enabled or disabled.

Step 5 Click **Add Rule** to add a rule to this policy.

Step 6 In the Add NAT Policy Rule dialog box, enter the IP address of the ASA 1000V outside interface as a rule condition for Destination Match Conditions.

Step 7 Configure other options in the Add NAT Policy Rule dialog box as described in Add NAT Policy Rule Dialog Box, on page 97, then click **OK**.

Note If any of the IP address fields includes a range that starts or ends with the IP address of the outside interface of the ASA 1000V, an error message will be displayed that identifies an overlap with the ASA 1000V interface IP address.

Step 8 Click **OK**.

Configuring Packet Inspection Policies

enables you to configure policies for application-layer protocol inspection. Inspection is required for services that embed IP addressing information in the user data packet, or that open secondary channels on dynamically assigned ports. When inspection is configured, the end device performs a deep packet inspection instead of quickly passing the packet on. As a result, inspection can affect overall device throughput.

Protocols Supported for Packet Inspection Policies, on page 102 lists the application-layer protocols supported by .

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policies > Packet Inspection**.
2. In the General tab, click **Add Packet Inspection Policy**.
3. In the Add Packet Inspection Policy dialog box, enter a name and description for the policy.
4. In the Admin State field, indicate whether the administrative status of the policy is enabled or disabled.
5. To add a rule to the policy, click **Add Rule**.
6. In the Add Packet Inspection Policy Rule Dialog box, provide the information as described in Add Packet Inspection Policy Rule Dialog Box, on page 102, then click **OK** in the open dialog boxes.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policies > Packet Inspection**.

Step 2 In the General tab, click **Add Packet Inspection Policy**.

Step 3 In the Add Packet Inspection Policy dialog box, enter a name and description for the policy.

Step 4 In the Admin State field, indicate whether the administrative status of the policy is enabled or disabled.

Step 5 To add a rule to the policy, click **Add Rule**.

Step 6 In the Add Packet Inspection Policy Rule Dialog box, provide the information as described in Add Packet Inspection Policy Rule Dialog Box, on page 102, then click **OK** in the open dialog boxes.

Protocols Supported for Packet Inspection Policies

CTIQBE	ICMP	PPTP	SQL *Net
DCE/RPC	ICMP Error	RSH	SunRPC
DNS	ILS	RSTP	TFTP
FTP	IP Options	SIP	WAAS
H323 H225	IPsec Pass-Through	Skinny	XDMCP
H323 RAS	MGCP	SMTP	
HTTP	NetBIOS	SNMP	

Add Packet Inspection Policy Rule Dialog Box

Field	Description
Name	Rule name.
Description	Brief rule description.
Action	Under Enable Inspections, check the check boxes of protocols to be inspected if the rule conditions are met.
Protocol	Not available for configuration.
Source Conditions	
Destination Conditions	

Configuring Routing Policies

enables you to use routing policies to configure static, OSPF, and BGP routes for managed resources.

Note You can configure only inside and outside interfaces on edge firewalls by using . Use the CLI to configure routes on the edge firewall management interface.

After you configure a static route routing policy, you can implement the policy by:

- Including the routing policy in an edge device profile.
- Applying the edge device profile to an edge firewall that has managed endpoints.

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policies > Routing**.
2. In the General tab, click **Add Routing Policy**.
3. In the Add Routing Policy dialog box, enter a name and brief description for the routing policy.
4. To add a new static route, click **Add Static Route**.
5. In the Add Static Route dialog box, enter the following information:
6. Click **OK**.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policies > Routing**.

Step 2 In the General tab, click **Add Routing Policy**.

Step 3 In the Add Routing Policy dialog box, enter a name and brief description for the routing policy.

Step 4 To add a new static route, click **Add Static Route**.

Step 5 In the Add Static Route dialog box, enter the following information:

a) In the Destination Network fields, enter the IP route prefix and prefix mask for the destination.

b) In the Forwarding (Next Hop) fields, enter the IP address of the next hop that can be used to reach the destination network.

Note The Forwarding Interface field applies only to ASA 1000V data interfaces. Use the CLI to configure routes on the ASA 1000V management interface.

c) (Optional) In the Distance Metric field, enter the distance metric.

Step 6 Click **OK**.

Configuring TCP Intercept Policies

enables you to configure TCP intercept policies that you can then associate with an edge security profile. TCP intercept policies that you associate with a device via an edge security profile are applied to all traffic on the outside interface of the device.

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policies > TCP Intercept**.
2. In the General tab, click **Add TCP Intercept Policy**.
3. In the Add TCP Intercept Policy dialog box, enter a name and brief description for the policy.
4. In the Admin State field, indicate whether the administrative status of the policy is to be enabled or disabled.
5. To add a rule to the policy, click **Add Rule**.
6. In the Add TCP Intercept Policy Rule dialog box, provide the information as described in Add TCP Intercept Policy Rule Dialog Box, on page 104.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policies > TCP Intercept**.

Step 2 In the General tab, click **Add TCP Intercept Policy**.

Step 3 In the Add TCP Intercept Policy dialog box, enter a name and brief description for the policy.

Step 4 In the Admin State field, indicate whether the administrative status of the policy is to be enabled or disabled.

Step 5 To add a rule to the policy, click **Add Rule**.

Step 6 In the Add TCP Intercept Policy Rule dialog box, provide the information as described in Add TCP Intercept Policy Rule Dialog Box, on page 104.

Add TCP Intercept Policy Rule Dialog Box

Field	Description
Name	Rule name.
Description	Brief rule description.
Maximum Number of Embryonic TCP Connections (0-65535)	Number of embryonic TCP connections allowed overall and per client: 1 In the Total field, enter the maximum number of embryonic TCP connections allowed. 2 In the client field, enter the maximum number of embryonic TCP connections allowed per client. The default value 0 (zero) indicates unlimited connections.
Protocol	Not available for configuration.
Source Conditions	Not available for configuration.
Destination Conditions	Not available for configuration.

Configuring Site-to-Site IPsec VPN Policies

enables you to configure site-to-site IPsec VPNs. In addition, you can configure a crypto map policy and attach it to an edge profile. For ease of configuration and to keep logical IPsec entities separate, configuration is divided into the following sections:

- Configuring Crypto Map Policies
- Configuring IKE Policies
- Configuring Interface Policy Sets
- Configuring IPsec Policies
- Configuring Peer Authentication Policies
- Configuring VPN Device Policies

To access VPN policies, choose **Policy Management > Service Policies > root > Policies > VPN.**

Configuring Crypto Map Policies

enables you to create crypto map policies that include:

- Rules for source and destination conditions.
- IP Security (IPsec) options, including an IPsec policy.
- Internet Key Exchange (IKE) options, including a peer device.

Crypto map policies are applied to interfaces by means of their inclusion in interface policy sets and edge security policies.

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policies > VPN > Crypto Map Policies**.
2. In the General tab, click **Add Crypto Map Policy**.
3. In the Add Crypto Map Policy dialog box, provide the information as described in Add Crypto Map Policy Dialog Box, on page 106, then click **OK**.
4. To add a policy rule, click **Add Rule** in the General tab and provide the required information as described in Add Crypto Map Policy Rule Dialog Box, on page 107.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policies > VPN > Crypto Map Policies**.

Step 2 In the General tab, click **Add Crypto Map Policy**.

Step 3 In the Add Crypto Map Policy dialog box, provide the information as described in Add Crypto Map Policy Dialog Box, on page 106, then click **OK**.

Step 4 To add a policy rule, click **Add Rule** in the General tab and provide the required information as described in Add Crypto Map Policy Rule Dialog Box, on page 107.

Add Crypto Map Policy Dialog Box

Field	Description
General Tab	
Name	Policy name.
Description	Brief policy description.
Admin State	Whether the administrative status of the policy is enabled or disabled.
Rule Table	
Add Rule	Click **Add Rule** to add a new rule to the current policy.
IPsec Settings Tab	
SA Lifetime	Length of time (in days, hours, minutes, and seconds) that a security association (SA) lives before expiring.
SA Lifetime Traffic (KB)	Volume of traffic, in kilobytes, that can pass between IPsec peers using a given SA before that association expires.
Enable Perfect Forwarding Secrecy	Whether or not Perfect Forward Secrecy (PFS) is enabled. PFS is a cryptographic characteristic associated with a derived shared secret value. With PFS, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys.
Diffie-Hellman Group	Available if PFS is enabled. Choose the Diffie-Hellman (DH) group for this policy: • Group 1—The 768-bit DH group. • Group 2—The 1024-bit DH group. • Group 5—The 1536-bit DH group.
IPsec Policies	The IPsec policy that applies to the current policy. Select an existing IPsec policy or click **Add IPsec Policy** to create a new policy.

Field	Description
Peer Device	Peer device. Choose an existing peer or click **Add Peer Device** to add a new peer. In the Add Peer Device dialog box, enter the peer device IP address or hostname.
Other Settings Tab	
Enable NAT Traversal	Whether or not IPsec peers can establish a connection through a NAT device.
Enable Reverse Route Injection	Whether or not static routes are automatically added to the routing table and then announced to neighbors on the private network.
Connection Type	Connection type for this policy: • Answer-Only—Responds only to inbound IKE connections during the initial proprietary exchange to determine the appropriate peer to which to connect. • Bidirectional—Accepts and originates connections based on this policy. • Originate-Only—Initiates the first proprietary exchange to determine the appropriate peer to which to connect.
Negotiation Mode	Mode to use for exchanging key information and setting up SAs: • Aggressive Mode—Faster mode, using fewer packets and exchanges, but does not protect the identity of the communicating parties. • Main Mode—Slower mode, using more packets and exchanges, but protects the identities of the communicating parties.
DH Group for Aggressive Mode	DH group to use when in aggressive mode: Group 1, Group 2, or Group 5.

Add Crypto Map Policy Rule Dialog Box

Field	Description
Name	Rule name.
Description	Brief rule description.
VPN Action	Action to take based on this rule: Permit or Deny.

Field	Description
Protocol	Protocols to examine for this rule: • To examine all protocols, check the **Any** check box. • To examine specific protocols: **1** Uncheck the **Any** check box. **2** From the Operator drop-down list, choose a qualifier: Equal, Not equal, Member, Not Member, In range, or Not in range. **3** In the Value fields, specify the protocol, object group, or range.
Source Conditions	Source attributes that must be matched for the rule to apply. To add a new condition, click **Add Rule Condition**. Available source attributes are IP Address and Network Port.
Destination Conditions	Destination attributes that must be matched for the rule to apply. To add a new condition, click **Add Rule Condition**. Available destination attributes are IP Address and Network Port.

Configuring IKE Policies

The Internet Key Exchange (IKE) protocol is a hybrid protocol that implements Oakley and SKEME key exchanges inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. The initial IKE implementation used the IPsec protocol, but IKE can be used with other protocols. IKE provides authentication of the IPsec peers, negotiates IPsec keys, and negotiates the IPsec Security Associations (SAs).

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policies > VPN > IKE Policies**.
2. In the General tab, click **Add IKE Policy**.
3. In the Add IKE Policy dialog box, enter a name and description for the policy.
4. Configure either an IKE V1 or IKE V2 policy:
   - IKE V1 Policy
     1. Click **Add IKE V1 Policy**.
     2. In the Add IKE V1 Policy dialog box, provide the information described in IKE V1 Policy Dialog Box, on page 110, then click **OK**.
   - IKE V2 Policy
     1. Click **Add IKE V2 Policy**.
     2. In the Add IKE V2 Policy dialog box, provide the information described in IKE V2 Policy Dialog Box, on page 110, then click **OK**.
5. Click **OK**.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policies > VPN > IKE Policies**.

Step 2 In the General tab, click **Add IKE Policy**.

Step 3 In the Add IKE Policy dialog box, enter a name and description for the policy.

Step 4 Configure either an IKE V1 or IKE V2 policy:

- IKE V1 Policy
  1. Click **Add IKE V1 Policy**.
  2. In the Add IKE V1 Policy dialog box, provide the information described in IKE V1 Policy Dialog Box, on page 110, then click **OK**.
- IKE V2 Policy
  1. Click **Add IKE V2 Policy**.
  2. In the Add IKE V2 Policy dialog box, provide the information described in IKE V2 Policy Dialog Box, on page 110, then click **OK**.

Step 5 Click **OK**.

IKE V1 Policy Dialog Box

Field	Description
DH Group	Diffie-Hellman group: Group 1, Group 2, or Group 5.
Encryption	Encryption method: 3DES, AES, AES-192, AES-256, or DES.
Hash	Hash algorithm: MD5 or SHA.
Authentication	Authentication method is Preshared key.
SA Lifetime	Length of time (in days, hours, minutes, and seconds) that an SA lives before expiring.

IKE V2 Policy Dialog Box

Field	Description
DH Group	Diffie-Hellman group: Group 1, Group 2, Group 5, or Group 14.
Encryption	Encryption method: 3DES, AES, AES-192, AES-256, or DES.
Hash	Hash integrity algorithm: MD5, SHA, SHA256, SHA384, or SHA512.
Pseudo Random Function Hash	Pseudo-random function (PRF) has algorithm: MD5, SHA, SHA256, SHA384, or SHA512.
SA Lifetime	Length of time (in days, hours, minutes, and seconds) that an SA lives before expiring.

Configuring Interface Policy Sets

Interface policy sets enable you to group multiple policies for inclusion in an edge security profile.

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policies > VPN > Interface Policy Sets**.
2. In the General tab, click **Add Interface Policy Set**.
3. In the Add Interface Policy Set dialog box, provide the information as described in Add Interface Policy Set Dialog Box, on page 111, then click **OK**.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policies > VPN > Interface Policy Sets**.

Step 2 In the General tab, click **Add Interface Policy Set**.

Step 3 In the Add Interface Policy Set dialog box, provide the information as described in Add Interface Policy Set Dialog Box, on page 111, then click **OK**.

Add Interface Policy Set Dialog Box

General Tab

Field	Description
Name	Policy set name.
Description	Brief description of the policy set.
Admin State	Administrative state of the policy set: enabled or disabled.
Policies Area	
Add Crypto Map Policy	Click to add a new policy.
Available	Policies that can be assigned to the policy set. Use the arrows between the columns to move policies between columns.
Assigned	Policies assigned to the policy set.
Up and down arrows	Changes the priority of the selected policies. Arrange the policies from highest to lowest priority, with the highest priority policy at the top of the list.

Domain Settings Tab

Field	Description
Enable IKE (Must check at least one)	Check the appropriate check box to specify IKE V1 or IKE V2.
Enable IPsec Pre-fragmentation	Check the check box to fragment packets before encryption. Pre-fragmentation minimizes post-fragmentation (fragmentation after encryption) and the resulting reassembly before decryption, thereby improving performance.

Field	Description
Do Not Fragment	Available only if the Enable IPsec Pre-fragmentation check box is checked. From the drop-down list, choose the action to take with the Don't Fragment (DF) bit in the encapsulated header: • Clear • Copy • Set

Configuring IPsec Policies

IPsec policies define the IPsec policy objects used to create a secure IPsec tunnel for a VPN.

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policies > VPN > IPsec Policies**.
2. In the General tab, click **Add IPsec Policy**.
3. In the Add IPsec Policy dialog box, enter a name and description for the policy.
4. To configure an IKE V1 proposal:
5. To configure an IKE V2 proposal:
6. Click **OK** to save the policy.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policies > VPN > IPsec Policies**.

Step 2 In the General tab, click **Add IPsec Policy**.

Step 3 In the Add IPsec Policy dialog box, enter a name and description for the policy.
You must configure ethier an IKE V1 or IKE V2 proposal for an IPsec policy.

Step 4 To configure an IKE V1 proposal:

a) In the IKE v1 Proposal Table area, click **Add IPsec IKEv1 Proposal**.
b) In the IPsec IKEv1 Proposal dialog box, provide the information described in IPsec IKEv1 Proposal Dialog Box, on page 113, then click **OK**.

Step 5 To configure an IKE V2 proposal:

a) In the IKE v2 Proposal Table area, click **Add IPsec IKE v2 Proposal**.
b) In the IPsec IKEv2 Proposal dialog box, provide the information described in IPsec IKEv2 Proposal Dialog Box, on page 114, then click **OK**.

Step 6 Click **OK** to save the policy.

IPsec IKEv1 Proposal Dialog Box

Field	Description
Mode	Mode in which the IPsec tunnel operates. In Tunnel mode, the IPsec tunnel encapsulates the entire IP packet.
ESP Encryption	Encapsulating Security Protocol (ESP) encryption method: • 3DES—Encrypts three times according to the Data Encryption Standard (DES) using 56-bit keys. • AES—Encrypts according to the Advanced Encryption Standard (AES) using 128-bit keys. • AES-192—Encrypts according to the AES using 192-bit keys. • AES-256—Encrypts according to the AES using 256-bit keys. • DES—Encrypts according to the DES using 56-bit keys. • Null—Null encryption algorithm. Transform sets defined with ESP-Null provide authentication without encryption; this method is typically used for testing purposes only.
ESP Authentication	Hash authentication algorithm: • MD5—Produces a 128-bit digest. • Null—Does not perform authentication. • SHA—Produces a 160-bit digest.

IPsec IKEv2 Proposal Dialog Box

Field	Description
ESP Encryption Algorithm Table	To add an ESP encryption method: **1** Click **Add ESP Encryption Algorithm**. **2** From the ESP Encryption drop-down list, choose the encryption method: • 3DES—Encrypts three times according to the Data Encryption Standard (DES) using 56-bit keys. • AES—Encrypts according to the Advanced Encryption Standard (AES) using 128-bit keys. • AES-192—Encrypts according to the AES using 192-bit keys. • AES-256—Encrypts according to the AES using 256-bit keys. • DES—Encrypts according to the DES using 56-bit keys. • Null—Null encryption algorithm. Transform sets defined with ESP-Null provide authentication without encryption; this method is typically used for testing purposes only.
Integrity Algorithm Table	To add an integrity algorithm: **1** Click **Add Integrity Algorithm**. **2** From the Integrity Algorithm drop-down list, choose the authentication algorithm: • MD5—Produces a 128-bit digest. • Null—Does not perform authentication. • SHA—Produces a 160-bit digest.

Configuring Peer Authentication Policies

Use a peer authentication policy to define the method used to authenticate a peer.

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policies > VPN > Peer Authentication Policies**.
2. In the General tab, click **Add Peer Authentication Policy**.
3. In the Add Peer Authentication Policy dialog box, enter a name and description for the policy.
4. Click **Add Policy to Authenticate Peer**.
5. In the Add Policy to Authenticate Peer dialog box, provide the information described in Add Policy to Authenticate Peer Dialog Box, on page 115, then click **OK**.
6. Click **OK** to save the policy.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policies > VPN > Peer Authentication Policies**.

Step 2 In the General tab, click **Add Peer Authentication Policy**.

Step 3 In the Add Peer Authentication Policy dialog box, enter a name and description for the policy.

Step 4 Click **Add Policy to Authenticate Peer**.

Step 5 In the Add Policy to Authenticate Peer dialog box, provide the information described in Add Policy to Authenticate Peer Dialog Box, on page 115, then click **OK**.

Step 6 Click **OK** to save the policy.

Add Policy to Authenticate Peer Dialog Box

Field	Description
Peer Device (Unique)	Unique IP address or hostname of the peer.
IKEv1 Area	
Local	Preshared key.
Confirm	Preshared key for confirmation.
Set	Whether or not the preshared key has been set and is properly configured (read-only).
IKEv2 Area	
Local	Local preshared key.
Confirm	Local preshared key for confirmation.
Set	Whether or not the local preshared key has been set and is properly configured (read-only).

Field	Description
Remote	Remote preshared key.
Confirm	Remote preshared key for confirmation.
Set	Whether or not the remote preshared key has been set and is properly configured (read-only).

Configuring VPN Device Policies

A VPN device policy enables you to specify VPN global settings, such as:

- IKE policy
- IKE global settings
- IPsec global settings
- Peer authentication policy

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policies > VPN > VPN Device Policies**.
2. In the General tab, click **Add VPN Device Policy**.
3. In the Add VPN Device Policy dialog box, provide the information as described in Add VPN Device Policy Dialog Box, on page 117.
4. As needed, provide the information described in the following tables:
5. Click **OK** to create the policy.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policies > VPN > VPN Device Policies**.

Step 2 In the General tab, click **Add VPN Device Policy**.

Step 3 In the Add VPN Device Policy dialog box, provide the information as described in Add VPN Device Policy Dialog Box, on page 117.

Step 4 As needed, provide the information described in the following tables:

- Configuring IKE Policies, on page 108
- Configuring Peer Authentication Policies, on page 114

Step 5 Click **OK** to create the policy.

Add VPN Device Policy Dialog Box

General Tab

Note A VPN device policy requires both an IKE policy and a peer authentication policy.

Field	Description
Name	Policy name.
Description	Brief policy description.
IKE Policy	Choose an existing policy from the drop-down list, or click **Add IKE Policy** to add a new policy.
Peer Authentication Policy	Choose an existing policy from the drop-down list, or click **Add Peer Authentication Policy** to add a new policy.

IKE Settings Tab

Field	Description
Enable IPsec over TCP	Whether or not IPsec traffic is allowed over TCP. If IPsec over TCP is enabled, this method takes precedence over all other connection methods.
Send Disconnect Notification	Whether or not clients are notified that sessions will be disconnected.
Allow Inbound Aggressive Mode	Whether or not inbound aggressive mode is permitted.
Wait for Termination before Rebooting	Whether or not a reboot can occur only when all active sessions have terminated voluntarily.
Threshold for Cookie Challenge (0-100 Percent)	Percentage of the maximum number of allowed Security Associations (SAs) that can be in-negotiation (open) before cookie challenges are issued for future SA negotiations.
Negotiation Threshold for Maximum SAs (0-100 Percent)	Percentage of the maximum number of allowed SAs that can be in-negotiation before additional connections are denied. The default value is 100 percent.

Field	Description
IKE Identity	Phase 2 identification method: • Automatic—Determines ISAKMP negotiation by connection type: ◦ IP address for a preshared key. ◦ Cert DN for certificate authentication. • IP Address—IP address of the host exchanging ISAKMP identity information. • Hostname—Fully qualified domain name of the host exchanging ISAKMP identity information. • Key ID—String used by the remote peer to look up the preshared key.
Key for IKE Identity	The key to use for IKE identify if the IKE identification method is Key ID.
NAT Traversal	Whether or not IPsec peers can establish a connection through a NAT device.
Keep-Alive Time for NAT Traversal	Length of time (in hours, minutes, and seconds) that a tunnel can exist with no activity before the device sends keepalive messages to the peer. Values range from 10 to 3600 seconds, with a default of 20 seconds.
IKEv2 IPsec Maximum Security Associations	Whether or not the total number of IKE V2 SAs on the node can be set.
Maximum Number of SA	Maximum number of SA connections allowed.
IKEv1 over TCP Port Table	1 Click **Add IKE V1 Over TCP Port** to add a new port. 2 In the Port field, enter the TCP port to use for IKE V1.

IPsec Settings Tab

Field	Description
Anti Replay	Whether or not SA anti-replay is enabled.

Field	Description
Anti Replay Window Size	Window size to use to track and prevent duplication of packets. Using a larger window size allows the decryptor to track more packets.
SA Lifetime	Length of time (in days, hours, minutes, and seconds) that an SA can live before expiring.
SA Lifetime Volume (KB)	Volume of traffic, in kilobytes, that can pass between IPsec peers using a given SA before the association expires.

Configuring Zone-Based Firewall Policies

A zone policy defines the traffic that you want to allow or deny between zones. A zone-pair policy allows you to specify a unidirectional firewall policy between two zones. The direction is defined by specifying a source and destination zone.

A firewall zone is a group of interfaces to which a policy can be applied. By default, traffic can flow freely within that zone but all traffic to and from that zone is dropped. To allow traffic to pass between zones, you must explicitly declare it by creating a zone-pair and a policy for that zone.

This workflow is part of the Edge Router Configuration Workflow, on page 211.

For more information on Zone Based Firewall policies and options, see http://www.cisco.com/en/US/partner/products/sw/secursw/ps1018/products_tech_note09186a00808bc994.shtml.

SUMMARY STEPS

1. Choose **Policy Management > Service Policies >** ***tenant*** **> Policies** and select **Zone Based Firewall**.
2. Choose **Zone Pair Policies** and add a zone pair policy. In this step you designate a source and destination zone and apply a policy map. If you have not configured a policy map, you can create one now and also configure associated class maps and rules.
3. Choose **Policy Sets** and create a policy set by identifying zone pair policies.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies >** ***tenant*** **> Policies** and select **Zone Based Firewall**.

Step 2 Choose **Zone Pair Policies** and add a zone pair policy. In this step you designate a source and destination zone and apply a policy map. If you have not configured a policy map, you can create one now and also configure associated class maps and rules.

Step 3 Choose **Policy Sets** and create a policy set by identifying zone pair policies.

Working with Profiles

A profile is a collection of policies. By creating a profile with policies that you select, and then applying that profile to multiple objects, such as edge firewalls, you can ensure that those objects have consistent policies.

A device must be registered to before you can apply a profile to it.

enables you to create and apply the following types of profiles:

- Compute security profiles—Compute firewall profiles that include ACL policies and user-defined attributes.
- Edge device profiles—Edge firewall profiles that include routing, VPN, DHCP, and IP Audit policies.
- Edge security profiles—Edge firewall profiles that include access and threat mitigation policies.

The following topics describe how to configure and apply profiles.

Configuring Compute Security Profiles

enables you to create compute security profiles at the root or tenant level. Creating a compute security profile at the root level enables you to apply the same profile to multiple tenants.

SUMMARY STEPS

1. Choose **Policy Management > Service Profiles > root > Compute Firewall > Compute Security Profiles**.
2. In the General tab, click **Add Compute Security Profile**.
3. In the Add Compute Security Profile dialog box, provide the information as described in Add Compute Security Profile Dialog Box, on page 121, then click **OK**.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Profiles > root > Compute Firewall > Compute Security Profiles**.

Step 2 In the General tab, click **Add Compute Security Profile**.

Step 3 In the Add Compute Security Profile dialog box, provide the information as described in Add Compute Security Profile Dialog Box, on page 121, then click **OK**.

Add Compute Security Profile Dialog Box

General Tab

Field	Description
Name	Profile name. This name can be between 2 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, period, and colon. You cannot change this name after it is saved.
Description	Brief profile description. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, period, and colon.
Policy Set	Drop-down list of policy sets.
Add ACL Policy Set	Click the link to add an ACL policy set.
Resolved Policy Set	Click the link to edit the resolved policy set.
Resolved Policies Area	
(Un)assign Policy	Click the link to assign or unassign a policy.
Name	Rule name.
Source Condition	Source condition for the rule.
Destination Condition	Destination condition for the rule.
Service/Protocol	Service or protocol to which the rule applies.
EtherType	Encapsulated protocol to which the rule applies.
Action	Action to take if the rule conditions are met.
Description	Rule description.

Attributes Tab

Field	Description
Add User Defined Attribute	Opens a dialog box for adding an attribute.
Name	Attribute name.
Value	Attribute value.

Verifying Compute Firewall Policies

Use this procedure to verify active policies and optionally modify policy objects for compute firewalls.

SUMMARY STEPS

1. Choose **Resource Management > Managed Resources > root >** *tenant* **> Compute Firewalls >** *compute-firewall*.
2. In the Compute Security Profiles tab, select the required policy, then click **Show Resolved Policies**.
3. In the Edit dialog box, click the required policy in the Resolved Policies table to view the policy details, such as source and destination conditions.
4. To modify a policy, in the Policy Set area, either choose a different policy from the drop-down list, or click **Add ACL Policy Set** to configure a new policy.
5. Click **Apply** to accept any changes or **OK** when you have finished reviewing the policies.

DETAILED STEPS

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant* **> Compute Firewalls >** *compute-firewall*.

Step 2 In the Compute Security Profiles tab, select the required policy, then click **Show Resolved Policies**.

Step 3 In the Edit dialog box, click the required policy in the Resolved Policies table to view the policy details, such as source and destination conditions.

Step 4 To modify a policy, in the Policy Set area, either choose a different policy from the drop-down list, or click **Add ACL Policy Set** to configure a new policy.

Step 5 Click **Apply** to accept any changes or **OK** when you have finished reviewing the policies.

Configuring Edge Device Profiles

Edge device profiles contain the following policies in addition to a timeout value for address translation:

- DHCP
- IP audit signature
- Routing
- VPN device

You can create an edge device profile at any level of the organization hierarchy (root, tenant, virtual data center (VDC), app, or tier). Creating an edge device profile at the root level enables you to apply it to multiple edge firewalls for different tenants.

SUMMARY STEPS

1. Choose **Policy Management > Service Profiles > root > Edge Firewall > Edge Device Profiles**.
2. In the General tab, click **Add Edge Device Profile**.
3. In the Add Edge Device Profile dialog box, enter the information as described in Edge Device Profile Dialog Box, on page 123, then click **OK**.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Profiles > root > Edge Firewall > Edge Device Profiles**.

Step 2 In the General tab, click **Add Edge Device Profile**.

Step 3 In the Add Edge Device Profile dialog box, enter the information as described in Edge Device Profile Dialog Box, on page 123, then click **OK**.

Edge Device Profile Dialog Box

Field	Description
General Tab	
Name	Profile name.
Description	Brief profile description.
Policies Tab	
Routing Policy	Choose an existing policy or click **Add Routing Policy** to add a new policy. Click the Resolved Policy link to review or modify the assigned policy.
IP Audit Signature Policy	Choose an existing policy or click **Add IP Audit Signature Policy** to add a new policy. Click the Resolved Policy link to review or modify the assigned policy.
VPN Device Policy	Choose an existing policy or click **Add VPN Device Policy** to add a new policy. Click the Resolved Policy link to review or modify the assigned policy.
Address Translations Timeout	Length of time (in days, hours, minutes, and seconds) that a translation can remain unused before it expires.
DHCP Policy	
Edge DHCP Policy	Adds a DHCP policy.

Field	Description
Type	Type of DHCP service: relay or server.
Interface Name	Interface to which the DHCP policy is applied.
Server/Relay Policy	DHCP policy name.

Configuring Edge Security Profiles

Edge security profiles can include any of the following:

- ACL policy sets (ingress and egress)
- Connection timeout policies
- IP audit policies
- NAT policy sets
- Packet inspection policies
- TCP intercept policies
- VPN interface policy sets

You can create an edge security profile at any level of the organizational hierarchy (root, tenant, VDC, app, or tier). Creating an edge security profile at the root level enables you to apply it to multiple edge firewalls for different tenants.

SUMMARY STEPS

1. Choose **Policy Management > Service Profiles > Edge Firewall > Edge Security Profiles**.
2. In the General tab, click **Add Edge Security Profile**.
3. In the Add Edge Security Profile dialog box provide the information as described in Add Edge Security Profile Dialog Box, on page 125.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Profiles > Edge Firewall > Edge Security Profiles**.

Step 2 In the General tab, click **Add Edge Security Profile**.

Step 3 In the Add Edge Security Profile dialog box provide the information as described in Add Edge Security Profile Dialog Box, on page 125.

Add Edge Security Profile Dialog Box

Field	Description
General Tab	
Name	Profile name.
Description	Brief profile description.
Ingress Tab	
Policy Set	Choose an existing policy set or click **Add ACL Policy Set** to add a new policy set. Click the **Resolved Ingress Policy Set** link to modify the assigned policy set.
Resolved Policies	Click **(Un)assign Policy** to assign or remove a policy for the current policy set.
Egress Tab	
Policy Set	Choose an existing policy set or click **Add ACL Policy Set** to add a new policy set. Click the **Resolved Egress Policy Set** link to modify the assigned policy set.
Resolved Policies	Click **(Un)assign Policy** to assign or remove a policy for the current policy set.
NAT Tab	
Policy Set	Choose an existing policy set or click **Add NAT Policy Set** to add a new policy set. Click the **Resolved NAT Policy Set** link to modify the assigned policy set.
Resolved Policies	Click **(Un)assign Policy** to assign or remove a policy for the current policy set.
VPN Tab	
Policy Set	Choose an existing policy set or click **Add Interface Policy Set** to add a new policy set. Click the **Resolved VPN Interface Policy Set** link to modify the assigned policy set.
Advanced Tab	

Field	Description
Packet Inspection Policy	Choose an existing policy or click **Add Packet Inspection Policy** to add a new policy. Click the **Resolved Policy** link to modify the assigned policy.
Connection Timeout Policy	Choose an existing policy or click **Add Connection Timeout Policy** to add a new policy. Click the **Resolved Policy** link to modify the assigned policy.
TCP Intercept Policy	Choose an existing policy or click **Add TCP Intercept Policy** to add a new policy. Click the **Resolved Policy** link to modify the assigned policy.
IP Audit Policy	Choose an existing policy or click **Add IP Audit Policy** to add a new policy. Click the **Resolved Policy** link to modify the assigned policy.

Applying an Edge Device Profile

After you have created an edge device profile, you can apply the profile to multiple edge firewalls to ensure consistent policies across the firewalls.

SUMMARY STEPS

1. Choose **Resource Management > Managed Resources > root >** *tenant* **> Edge Firewalls >** *edge-firewall*.
2. In the General tab, click **Select** in the Edge Device Profile field.
3. In the Select Edge Device Profile dialog box, select the required profile, then click **OK**.
4. Click **Save**.

DETAILED STEPS

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant* **> Edge Firewalls >** *edge-firewall*.

Step 2 In the General tab, click **Select** in the Edge Device Profile field.

Step 3 In the Select Edge Device Profile dialog box, select the required profile, then click **OK**.

Step 4 Click **Save**.

Applying an Edge Security Profile

After you have created an edge security profile, you can apply it to edge firewall instances to ensure consistent policies on the interfaces.

Note Edge security profiles can be applied only on outside interfaces of edge firewalls.

SUMMARY STEPS

1. Choose **Resource Management > Managed Resources > root >** *tenant* **> Edge Firewalls >** *edge-firewall*.
2. In the Interfaces table, select the required outside interface, then click **Edit**.
3. In the Edit dialog box, click **Select** in the Edge Security Profile field.
4. In the Select Edge Security Profile dialog box, select the required profile, then click **OK**.
5. Click **OK** in the open dialog boxes, then click **Save**.

DETAILED STEPS

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant* **> Edge Firewalls >** *edge-firewall*.
Step 2 In the Interfaces table, select the required outside interface, then click **Edit**.
Step 3 In the Edit dialog box, click **Select** in the Edge Security Profile field.
Step 4 In the Select Edge Security Profile dialog box, select the required profile, then click **OK**.
Step 5 Click **OK** in the open dialog boxes, then click **Save**.

Verifying Edge Firewall Policies

Use this procedure to verify active policies and optionally modify policy objects for edge firewalls.

SUMMARY STEPS

1. Choose **Resource Management > Managed Resources > root >** *tenant* **> Edge Firewalls >** *edge-firewall*.
2. In the Edge Security Profiles tab, select the required policy, then click **Show Resolved Policies**.
3. To view policy or policy set details, use the tabs in the Edit dialog box to navigate to the required policy or policy set, then click the required policy or policy set in Resolved field
4. To use a different policy or policy set, navigate to the required policy or policy set, then either choose a different policy or policy set from the drop-down list, or add a new policy or policy set.
5. Click **Apply** to accept any changes or **OK** when you have finished reviewing the policies.

DETAILED STEPS

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant* **> Edge Firewalls >** *edge-firewall*.

Step 2 In the Edge Security Profiles tab, select the required policy, then click **Show Resolved Policies**.

Step 3 To view policy or policy set details, use the tabs in the Edit dialog box to navigate to the required policy or policy set, then click the required policy or policy set in Resolved field

Step 4 To use a different policy or policy set, navigate to the required policy or policy set, then either choose a different policy or policy set from the drop-down list, or add a new policy or policy set.

Step 5 Click **Apply** to accept any changes or **OK** when you have finished reviewing the policies.

Configuring Security Profiles

Editing a Security Profile for a Compute Firewall

SUMMARY STEPS

1. Choose **Policy Management > Service Profiles > root > Compute Firewalls > Compute Security Profiles**.
2. In the General tab, select the profile you want to edit, then click **Edit**.
3. In the Edit Compute Security Profile dialog box, edit the fields as required by using the information in the following tables, then click **OK**.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Profiles > root > Compute Firewalls > Compute Security Profiles**.

Step 2 In the General tab, select the profile you want to edit, then click **Edit**.

Step 3 In the Edit Compute Security Profile dialog box, edit the fields as required by using the information in the following tables, then click **OK**.

Field	Description
Name	Profile name.
Description	Brief policy description.
Policy Set	List of available policy sets.
Add ACL Policy Set	Click to add a new ACL policy set.
Resolved Policy Set	Click the link to view and optionally edit the resolved policy set.
Resolved Policies	

Field	Description
(Un)assigned Policy	Click to assign or unassign policies.
Name	Policy name.
Source Condition	Source condition for the policy.
Destination Condition	Destination condition for the policy.
Service/Protocol	Protocol specify by the policy.
EtherType	EtherType specified by the policy.
Action	Action to take if the specified condition is met.
Description	Brief policy description.

Field	Description
Add User Defined Attribute	Click to add a custom attribute.
Name	Attribute name.
Value	Attribute value.

Editing a Security Profile for an Edge Firewall

This procedure enables you to edit a security profile associated with an edge firewall.

SUMMARY STEPS

1. Choose **Policy Management > Service Profiles > root > Edge Firewall > Edge Security Profiles**.
2. In the General tab, select the edge security profile that you want to edit, then click **Edit**.
3. In the Edit Edge Security Profile dialog box, edit the entries as required by using the information in the following table, then click **OK**.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Profiles > root > Edge Firewall > Edge Security Profiles**.

Step 2 In the General tab, select the edge security profile that you want to edit, then click **Edit**.

Step 3 In the Edit Edge Security Profile dialog box, edit the entries as required by using the information in the following table, then click **OK**.

Field	Description
General Tab	
Name	Profile name (read-only).
Description	Brief profile description.
ID	Unique profile identifier (read-only).
Ingress Tab	
Policy Set	Choose an existing policy set or click **Add ACL Policy Set** to add a new policy set. Click the **Resolved Ingress Policy Set** link to modify the assigned policy set.
Resolved Policies	Click **(Un)assign Policy** to assign or remove a policy for the current policy set.
Egress Tab	
Policy Set	Choose an existing policy set or click **Add ACL Policy Set** to add a new policy set. Click the **Resolved Egress Policy Set** link to modify the assigned policy set.
Resolved Policies	Click **(Un)assign Policy** to assign or remove a policy for the current policy set.
NAT Tab	
Policy Set	Choose an existing policy set or click **Add NAT Policy Set** to add a new policy set. Click the **Resolved NAT Policy Set** link to modify the assigned policy set.
Resolved Policies	Click **(Un)assign Policy** to assign or remove a policy for the current policy set.
VPN Tab	
Policy Set	Choose an existing policy set or click **Add Interface Policy Set** to add a new policy set. Click the **Resolved VPN Interface Policy Set** link to modify the assigned policy set.

Field	Description
Advanced Tab	
Packet Inspection Policy	Choose an existing policy or click **Add Packet Inspection Policy** to add a new policy. Click the **Resolved Policy** link to modify the assigned policy.
Connection Timeout Policy	Choose an existing policy or click **Add Connection Timeout Policy** to add a new policy. Click the **Resolved Policy** link to modify the assigned policy.
Threat Migration	Choose an existing policy or click **Add TCP Intercept Policy** to add a new policy. Click the **Resolved Policy** link to modify the assigned policy.
IP Audit Policy	Choose an existing policy or click **Add IP Audit Policy** to add a new policy. Click the **Resolved Policy** link to modify the assigned policy.

Deleting a Security Profile

SUMMARY STEPS

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

DETAILED STEPS

Step 1 In the **Navigation** pane, choose **Policy Management** > **Security Policies**> **root** > **Security Profiles**.

Step 2 In the **Work** pane, click the security profile you want to delete.

Step 3 Click **Delete.**

Step 4 In the Confirm dialog box, click **OK**.

Deleting a Security Profile Attribute

SUMMARY STEPS

1. In the **Navigation** pane, choose **Policy Management > Security Profiles > root > Security Profiles** > *security profile*. The security profile is the profile that contains the attribute you want to delete.
2. In the **Work** pane, click the **Attributes** tab.
3. Click the attribute you want to delete.
4. Click **Delete.**
5. In the Confirm dialog box, click **OK**.

DETAILED STEPS

Step 1 In the **Navigation** pane, choose **Policy Management > Security Profiles > root > Security Profiles** > *security profile*. The security profile is the profile that contains the attribute you want to delete.

Step 2 In the **Work** pane, click the **Attributes** tab.

Step 3 Click the attribute you want to delete.

Step 4 Click **Delete.**

Step 5 In the Confirm dialog box, click **OK**.

Assigning a Policy

SUMMARY STEPS

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

DETAILED STEPS

Step 1 In the **Navigation** pane, expand **Policy Management** > **Security Profiles** > **root** > **Security Profiles**.

Step 2 Click the profile where you want to assign the policy.

Step 3 In the **Work** pane, click the **(Un)assign Policy** link.

Step 4 In the **(Un)assign Policy** dialog box, move the policy you want assigned to the **Assigned** list.

Step 5 Click **OK**.

Unassigning a Policy

SUMMARY STEPS

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

DETAILED STEPS

Step 1 In the **Navigation** pane, expand **Policy Management** > **Security Profiles** > **root** > **Security Profiles**.

Step 2 Click the profile where you want to unassign the policy.

Step 3 In the **Work** pane, click the **(Un)assign Policy** link.

Step 4 In the **(Un)assign Policy** dialog box, move the policy you want unassigned to the **Available** list.

Step 5 Click **OK**.

Configuring Security Policy Attributes

Configuring Object Groups

An object group defines a collection of condition expressions on a system-defined or user-defined attribute. An object group can be referred to in a policy rule condition when the member or not-member operator is selected. A rule condition that refers to an object group resolves to true if any of the expressions in the object group are true.

Object groups can be created at any level in the organizational hierarchy.

Adding an Object Group

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root >** *tenant* **> Policy Helpers > Object Groups**.
2. In the General tab, click **Add Object Group**.
3. In the Add Object Group dialog box, complete the following fields, then click **OK**:

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root >** *tenant* **> Policy Helpers > Object Groups**.

Step 2 In the General tab, click **Add Object Group**.

Step 3 In the Add Object Group dialog box, complete the following fields, then click **OK**:

Note You must specify an attribute type and name before adding an object group expression. With Hyper-V hypervisors, the attribute type VM is not supported and if you choose the attribute type Network, the attribute name Service is not supported.

Field	Description
Name	Object group name. This name can be between 2 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, period, and colon. You cannot change this name after it is saved.
Description	Brief description of the object group. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, period, and colon.
Attribute Type	Available attribute types: Network, VM, User Defined, vZone, and Time Range. You must configure an attribute type and name to add an object group expression.
Attribute Name	Available attribute names for the selected attribute type.
Expression Table	
Add Object Group Expression	Click to add an object group expression.
Operator	Operator for the selected expression.
Value	Value for the selected expression.

Adding an Object Group Expression

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policy Helpers > Object Groups**.
2. In the General tab, select the object group you want to add an object group expression to, then click **Edit**.
3. In the Edit Object Group dialog box, click **Add Object Group Expression**.
4. In the Add Object Group Expression dialog box, specify the object group expression by using the information in the following table, then click **OK** in the open dialog boxes.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policy Helpers > Object Groups**.

Step 2 In the General tab, select the object group you want to add an object group expression to, then click **Edit**.

Note For new object groups, you must specify the attribute type and name before adding an object group expression.

Step 3 In the Edit Object Group dialog box, click **Add Object Group Expression**.

Step 4 In the Add Object Group Expression dialog box, specify the object group expression by using the information in the following table, then click **OK** in the open dialog boxes.

Field	Description
Attribute Name	Attribute (read-only).
Operator	Available operators for this attribute.
Attribute Value	Attribute value for this expression.

Editing an Object Group

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root >** *tenant* **> Policy Helpers > Object Groups**.
2. In the General tab, select the object group you want to edit, then click **Edit**.
3. In the Edit Object Group dialog box, update the fields as follows, then click **OK** in the open dialog boxes:

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root >** *tenant* **> Policy Helpers > Object Groups**.

Step 2 In the General tab, select the object group you want to edit, then click **Edit**.

Step 3 In the Edit Object Group dialog box, update the fields as follows, then click **OK** in the open dialog boxes:

Field	Description
Name	Object group name (read-only).
Description	Object group description. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, period, and colon.
Attribute Type	Specified attribute type (read-only).

Field	Description
Attribute Name	Specified attribute name (read-only).
Expression Table	
Add Object Group Expression	Click to add a new object group expression.
Edit	Enables you to edit the selected object group expression.
Delete	Deletes the selected object group expression.
Operator	Expression operator.
Value	Expression attribute value.

Editing an Object Group Expression

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policy Helpers > Object Groups**.
2. In the General tab, select the object group with the expression you want to edit, then click **Edit**.
3. In the Expression table in the Edit Object Group dialog box, select the expression you want to edit, then click **Edit**.
4. In the Edit Object Group Expression dialog box, edit the fields as required, then click **OK** in the open dialog boxes.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policy Helpers > Object Groups**.

Step 2 In the General tab, select the object group with the expression you want to edit, then click **Edit**.

Step 3 In the Expression table in the Edit Object Group dialog box, select the expression you want to edit, then click **Edit**.

Step 4 In the Edit Object Group Expression dialog box, edit the fields as required, then click **OK** in the open dialog boxes.

Field	Description
Attribute Name	Attribute name (read-only).
Operator	Available operators for this expression.
Attribute Value	Attribute value for this expression.

Deleting an Object Group

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policy Helpers > Object Groups**.
2. In the General tab, select the Object Group you want to delete, then click **Delete**.
3. When prompted, confirm the deletion.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policy Helpers > Object Groups**.

Step 2 In the General tab, select the Object Group you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Deleting an Object Group Expression

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policy Helpers > Object Groups**.
2. In the General tab, select the object group that contains the expression you want to delete, then click **Edit**.
3. In the Edit Object Group dialog box, select the expression that you want to delete In the Expression table, then click **Delete**.
4. When prompted confirm the deletion.
5. Click **OK** in the open dialog box to save the change.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policy Helpers > Object Groups**.

Step 2 In the General tab, select the object group that contains the expression you want to delete, then click **Edit**.

Step 3 In the Edit Object Group dialog box, select the expression that you want to delete In the Expression table, then click **Delete**.

Step 4 When prompted confirm the deletion.

Step 5 Click **OK** in the open dialog box to save the change.

Configuring Security Profile Dictionary

Adding a Security Profile Dictionary

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root >** *tenant* **> Policy Helpers > Security Profile Dictionary**.
2. In the General tab, click **Add Security Profile Dictionary**.
3. In the Add Security Profile Dictionary dialog box, complete the following fields as appropriate, then click **OK**:

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root >** *tenant* **> Policy Helpers > Security Profile Dictionary**.

Step 2 In the General tab, click **Add Security Profile Dictionary**.

Step 3 In the Add Security Profile Dictionary dialog box, complete the following fields as appropriate, then click **OK**:

Field	Description
Name	Name of the security profile dictionary. This name can contain 1 to 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved. **Note** You can have one security profile dictionary at the root level and one for each tenant.
Description	A description of the security profile dictionary. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, period, and colon.
Attributes Table	
Add Security Profile Custom Attribute	Click to add a new attribute.
Name	Custom attribute name.
Description	Custom attribute description.

Adding a Security Profile Dictionary Attribute

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root >** *tenant* **> Policy Helpers > Security Profile Dictionary**.
2. In the General tab, select the security profile dictionary that you want to add an attribute to, then click **Edit**.
3. In the Edit Security Profile Dictionary dialog box, click **Add Security Profile Custom Attribute**.
4. In the Add Security Profile Custom Attribute dialog box, complete the following fields, then click **OK**:

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root >** *tenant* **> Policy Helpers > Security Profile Dictionary**.

Step 2 In the General tab, select the security profile dictionary that you want to add an attribute to, then click **Edit**.

Step 3 In the Edit Security Profile Dictionary dialog box, click **Add Security Profile Custom Attribute**.

Step 4 In the Add Security Profile Custom Attribute dialog box, complete the following fields, then click **OK**:

Field	Description
Name	Attribute name. 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 saved.
Description	Attribute description. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, period, and colon.

Editing a Security Profile Dictionary

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policy Helpers > Security Profile Dictionary**.
2. In the General tab, select the security profile dictionary you want to edit, then click **Edit**.
3. In the Edit Security Profile Dictionary dialog box, modify the fields as appropriate, then click **OK**:

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policy Helpers > Security Profile Dictionary**.

Step 2 In the General tab, select the security profile dictionary you want to edit, then click **Edit**.

Step 3 In the Edit Security Profile Dictionary dialog box, modify the fields as appropriate, then click **OK**:

Field	Description
Name	Name of the security profile dictionary (read-only).
Description	Description of the security profile dictionary.
Attributes	
Add Security Profile Custom Attribute	Click to add a custom attribute.
Name	Attribute name.
Description	Attribute description.

Editing a Security Profile Dictionary Attribute

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policy Helpers > Security Profile Dictionary**.
2. In the General tab, select the security profile dictionary that contains the attribute you want to edit, then click **Edit**.
3. In the Edit Security Profile Dictionary dialog box, select the attribute you want to edit, then click **Edit**.
4. In the Edit Security Custom Attribute dialog box, edit the Description field as required, then click **OK** in the open dialog boxes to save the change.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policy Helpers > Security Profile Dictionary**.

Step 2 In the General tab, select the security profile dictionary that contains the attribute you want to edit, then click **Edit**.

Step 3 In the Edit Security Profile Dictionary dialog box, select the attribute you want to edit, then click **Edit**.

Step 4 In the Edit Security Custom Attribute dialog box, edit the Description field as required, then click **OK** in the open dialog boxes to save the change.

Deleting a Security Profile Dictionary

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policy Helpers > Security Profile Dictionary**.
2. In the General tab, select the security profile dictionary you want to delete, then click **Delete**.
3. When prompted, confirm the deletion.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policy Helpers > Security Profile Dictionary**.

Step 2 In the General tab, select the security profile dictionary you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Deleting a Security Profile Dictionary Attribute

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policy Helpers > Security Profile Dictionary**.
2. In the Edit Security Profile Dictionary dialog box, in Attributes table, select the attribute you want to delete, then click **Delete**.
3. When prompted, confirm the deletion.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policy Helpers > Security Profile Dictionary**.
In the General tab, select the dictionary that contains the attribute you want to delete, then click **Edit**.

Step 2 In the Edit Security Profile Dictionary dialog box, in Attributes table, select the attribute you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Working with vZones

A virtual zone (vZone) is a logical grouping of VMs or hosts. vZones facilitate working with policies and profiles because vZones enable you to write policies based on vZone attributes by using vZone names.

The high level flow for working with vZones in is as follows:

1. Define a vZone, each with one or more conditions for inclusion in the vZone.

2. Define a service policy with the rules based on zone or network conditions.
3. Create a policy set that includes the service policy defined in Step 2.
4. Create a security profile that includes the policy set created in Step 3.
5. Bind the security profile to the ASA 1000V or VSG port profile.
6. Assign the security profile to the ASA 1000V or VSG in .

See the following topics for more information about working with vZones.

Adding a vZone

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policy Helpers > vZones**.
2. In the General tab, click **Add vZone**.
3. In the Add vZone dialog box provide the required information as described in the following table, then click **OK**:

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policy Helpers > vZones**.

Step 2 In the General tab, click **Add vZone**.

Step 3 In the Add vZone dialog box provide the required information as described in the following table, then click **OK**:

Field	Description
Name	vZone name. The name can be between 2 and 32 characters. You can use alphanumeric characters including hyphen, underscore, period, and colon. You cannot change the name after it is saved.
Description	vZone description. The description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, period, and colon.
Condition Match Criteria	Condition match options: • Choose match-all for the zone to match all the conditions (AND). • Choose match-any for the zone to match any one condition (OR).
vZone Condition	
Attribute Type	Condition type.
Attribute Name	Condition attribute name. **Note** vZone conditions cannot be created using the service attribute.
Operator	Condition operator.

Field	Description
Attribute Value	Condition attribute value.

Editing a vZone

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policy Helpers > vZones**.
2. In the General tab, select the vZone that you want to edit, then click **Edit**.
3. In the Edit vZone dialog box in the General tab, right-click the attribute that you want to edit, and choose **Edit**.
4. In the Edit Zone Condition dialog box, edit the fields as required, then click **OK** in the open dialog boxes.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policy Helpers > vZones**.

Step 2 In the General tab, select the vZone that you want to edit, then click **Edit**.

Step 3 In the Edit vZone dialog box in the General tab, right-click the attribute that you want to edit, and choose **Edit**.

Step 4 In the Edit Zone Condition dialog box, edit the fields as required, then click **OK** in the open dialog boxes.

Field	Description
Name	vZone name (read-only).
Description	Brief vZone description.
Condition Match Criteria	Choose the required match option: • Match-all—Match all of the criteria (AND). • Match-any—Match any one of the criteria (OR).
vZone Condition	
Toolbar	
Add Zone Condition	Adds a zone condition.
Edit	Enables you to edit the selected condition.
Delete	Deletes the selected condition.

Field	Description
Filter	Filters the contents by the string or value that you enter.
Table	
Attribute Name	Zone condition attribute name.
Operator	Zone condition operator.
Attribute Value	Value for the zone condition.

Deleting a vZone Condition

SUMMARY STEPS

1. Choose **Policy Management > Service Policies > root > Policy Helpers > vZones**.
2. In the General tab, select the vZone with the condition that you want to delete, then click **Edit**.
3. In the Edit vZone dialog box, select the condition in the vZone Condition table that you want to delete, then click **Delete**.
4. Confirm the deletion.
5. In the Edit vZone dialog box, click **OK** or **Apply**.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policy Helpers > vZones**.

Step 2 In the General tab, select the vZone with the condition that you want to delete, then click **Edit**.

Step 3 In the Edit vZone dialog box, select the condition in the vZone Condition table that you want to delete, then click **Delete**.

Step 4 Confirm the deletion.

Step 5 In the Edit vZone dialog box, click **OK** or **Apply**.

Deleting a vZone

SUMMARY STEPS

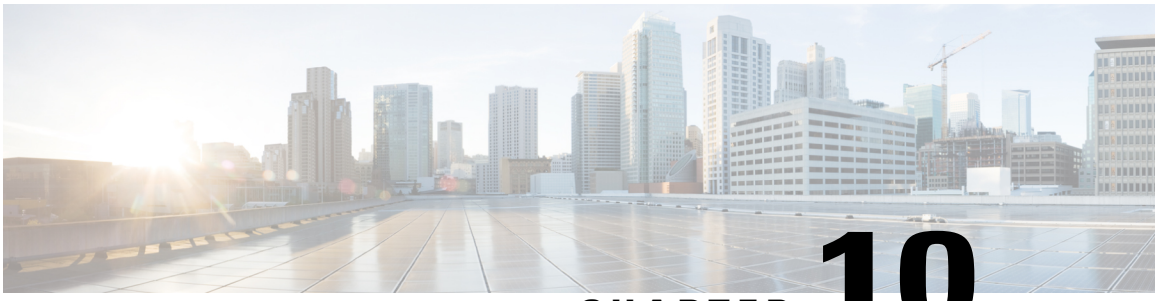
1. Choose **Policy Management > Service Policies > root > Policy Helpers > vZones**.
2. In the General tab, select the vZones that you want to delete, then click **Delete**.
3. Confirm the deletion.

DETAILED STEPS

Step 1 Choose **Policy Management > Service Policies > root > Policy Helpers > vZones**.

Step 2 In the General tab, select the vZones that you want to delete, then click **Delete**.

Step 3 Confirm the deletion.



CHAPTER 10

Configuring Device Policies and Profiles

This section includes the following topics:

- Device Policies and Profiles, page 147
- Device Configuration, page 148
- Device Policies, page 149
- Configuring Device Policies, page 149
- Configuring Device Profiles, page 185
- Configuring NTP, page 189
- Associating Device Policies with Profiles, page 192

Device Policies and Profiles

enables you to create device profiles and policies at any organizational level.

Device Profiles

A device profile is a set of custom security attributes and device policies. For Nexus 1000V VSMs, the device profile is added to the port profile. The port profile is assigned to the Nexus 1000V VSM vNIC, making the device profile part of the virtual machine (VM). Adding a device 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 apply device profiles by choosing Resource Management > Managed Resources and then navigating to the required device at the root or tenant level. The Firewall Settings area of the firewall pane includes the Device Profile option.

includes a default device profile at root level. The default device profile can be edited but cannot be deleted.

Policies

supports the following objects related to policies:

- Policy set—Contains policies. After a policy set is created, it can be assigned to a profile. An existing default policy set is automatically assigned at system boot up.
- Policy—Contains rules that can be ordered. An existing default policy is automatically assigned at system boot up. The default policy contains a rule with an action of **drop**.
- Rule—Contains conditions for regulating traffic. The default policy contains a rule with an action of **drop**. Conditions for a rule can be set using the network, custom, and virtual machine attributes.
- Object group—Can be created under an organization node. An object group defines a collection of condition expressions on a system-defined or user-defined attribute. An object group can be referred to in a policy rule condition when the member or not-member operator is selected. A rule condition that refers to an object group resolves to true if any of the expressions in the object group are true.
- Security Profile Dictionary—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 create only one dictionary for a tenant and one for 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. You cannot create a dictionary below the tenant level.
- Zone—Set of VMs based on conditions. The zone name is used in the authoring rules.

Security policies are created and then pushed to the Cisco VSG or ASA 1000V.

Device Configuration

enables you to configure devices by adding policies to a device profile and then applying that profile to a device. To create a root device profile, choose **Policy Management** > **Device Configurations** > **root** and click **Add Device Profile**. Device profiles contain options for the following policies and settings:

- DNS server and domain
- NTP server
- SNMP policy
- Syslog policy
- Fault policy
- Core policy
- Log file policy
- Policy engine logging
- Authentication policy
- Authorization Policy
- Accounting Policy

- Global Server Timers

Device Policies

enables you to create the following policies and assign them to device profiles for application to service devices:

- AAA policy
- Core file policy
- Fault policy
- Logging policy
- SNMP policy
- Syslog policy

provides default polices for fault, logging, SNMP, and syslog. The default policies cannot be deleted but can be modified. A device profile uses name resolution to resolve policy assignments. For details, see Name Resolution in a Multi-Tenant Environment, on page 66.

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

Configuring Device Policies

enables you to configure and manage the following types of device policies:

- AAA
- Core File
- Fault
- Log File
- SNMP
- Syslog

Configuring AAA Policies

Authentication, authorization, and accounting (AAA) policies verify users before they are allowed access to a network and network services. By creating AAA policies in and associating the policies with objects through device profiles, you can ensure that only authenticated users can access the objects.

Note Edge Firewall supports only Remote Access Method under Authentication Policy. Compute Firewall supports all the AAA policies.

supports authentication and authorization for edge firewalls, compute firewalls, and server groups using the following protocols:

- Kerberos
- Lightweight Directory Access Protocol (LDAP)
- RSA SecurID (SDI)

Note Cisco VSG Release 5.2(1)VSG2(2.0) and later releases support AAA with RADIUS and TACACS+ protocols.

You can use to configure an AAA policy on ASA 1000V. does not support AAA policies on VSG, VPX, or CSR 1000V.

SUMMARY STEPS

1. Choose **Policy Management** > **Device Configurations** > **root** > **Policies** > **AAA** > **Authentication Policies**.
2. In the General tab, click **Add Authentication Policy**.
3. In the Add Authentication Policy dialog box, enter the information as described in Add Authentication Policy Dialog Box, on page 151, then click **OK**.

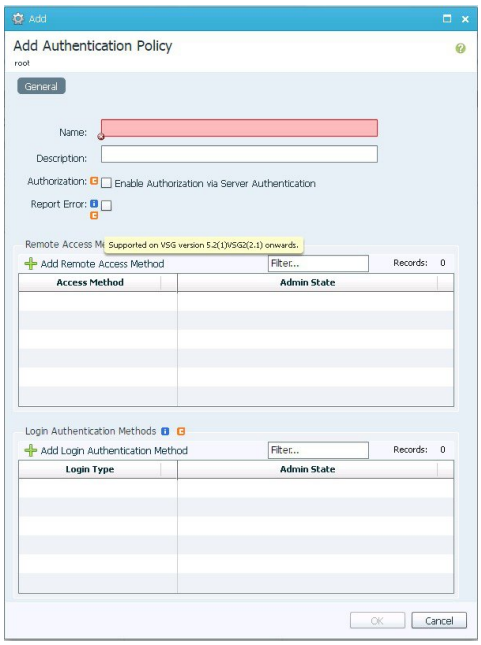
DETAILED STEPS

Step 1 Choose **Policy Management** > **Device Configurations** > **root** > **Policies** > **AAA** > **Authentication Policies**.

Step 2 In the General tab, click **Add Authentication Policy**.

Step 3 In the Add Authentication Policy dialog box, enter the information as described in Add Authentication Policy Dialog Box, on page 151, then click **OK**.

Figure 3: Add Authentication Policy Dialog Box



Note If you add a remote server group with a new server group with a new server host, the information that you must provide for the host depends on the protocol used. For example, the information required for a RADIUS server host is different from the information required for an LDAP server host. See the online help for the information required for the selected protocol.

Field Descriptions

Add Authentication Policy Dialog Box

Field	Description
Name	Policy name.
Description	Brief policy description.
Authorization	Check the Enable check box to enable authorization via server authentication. **Note** This option is not supported on Cisco VSG.
Remote Access Methods	

Field	Description
Add Remote Access Method	Adds a remote access method to the policy. For more information, see Remote Access Method Dialog Box, on page 152.
Access Method	One of the following access methods: • Enable Mode • HTTP • Serial • SSH • Telnet **Note** Starting with Cisco VSG Release 5.2.(1)VSG2(2.x), make sure that you define SSH Access Method for all the Remote Server Groups used for AAA Policies.
Admin State	Whether the administrative state of the policy is enabled or disabled.
Login Authentication Method	
Add Login Authentication Method	Adds a login method to the policy.
Login Type	One of the following login methods: • console • default
Admin State	Whether the administrative state of the policy is enabled or disabled.

Remote Access Method Dialog Box

Field	Description
Access Method	One of the following access methods: • Enable Mode • HTTP • Serial • SSH • Telnet **Note** Starting with Cisco VSG release 5.2(1)VSG2(2.0), only SSH is supported.

Field	Description
Admin State	Whether the administrative state of the access method is enabled or disabled.
Server Group	Select the server groups in "Available" Group and with the arrows buttons move them to "Assigned" Group.

Login Authentication Method Dialog Box

Note **Supported by Compute Firewall in Cisco VSG Release 5.2.(1)VSG2(2.0) and later releases.**

Field	Description
Login Type	One of the login methods: • console • default
Admin State	Whether the administrative state of the access method is enabled or disabled.
Server Group	Select the server groups in "Available" Group and with the arrows buttons move them to "Assigned" Group. **Note** Ensure that the SSH Access Method is defined for all the selected Server Groups .

Configuring Authorization Policies

Note Supported by Compute Firewall in Cisco VSG Release 5.2.(1)VSG2(2.x) onwards.

SUMMARY STEPS

1. Choose **Policy Management** > **Device Configurations** > **root** > **Policies** > **AAA** > **Authorization Policies**.
2. In the General tab, click **Add Authorization Policy**.
3. In the Add Authorization Policy dialog box, enter the information as described in following table, then click **OK**.

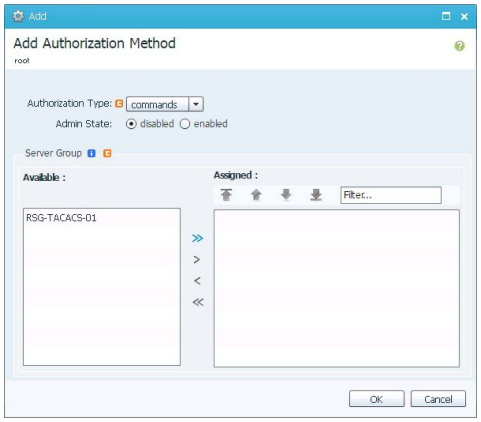
DETAILED STEPS

Step 1 Choose **Policy Management** > **Device Configurations** > **root** > **Policies** > **AAA** > **Authorization Policies**.

Step 2 In the General tab, click **Add Authorization Policy**.

Step 3 In the Add Authorization Policy dialog box, enter the information as described in following table, then click **OK**.

Figure 4: Add Authorization Method Dialog Box



Note If you add a remote server group with a new server host, the information that you must provide for the host depends on the protocol used. For example, the information required for a RADIUS server host is different from the information required for an LDAP server host. See the online help for the information required for the selected protocol.

Add Authorization Policy Dialog Box

Field	Description
Name	Policy name.
Description	A brief policy description.
Authorization Type	One of the following access methods: • commands • exec
Admin State	Whether the administrative state of the policy is enabled or disabled.

Authorization Method Dialog Box

Field	Description
Authorization Type	One of the login methods: • command • exec
Admin State	Whether the administrative state of the access method is enabled or disabled.
Server Group	Select the server groups in "Available" Group and with the arrows buttons move them to "Assigned" Group. **Note** Ensure that the SSH Access Method is defined for all the selected server Groups.

Configuring Accounting Policy

Note Supported only by Compute Firewall in Cisco VSG Release 5.2.(1)VSG2(2.x) and later releases.

SUMMARY STEPS

1. Choose **Policy Management** > **Device Configurations** > **root** > **Policies** > **AAA** > **Accounting Policies**.
2. In the General tab, click **Add Accounting Policy**.
3. In the Add Accounting Policy dialog box, enter the information as described in following table, then click **OK**.

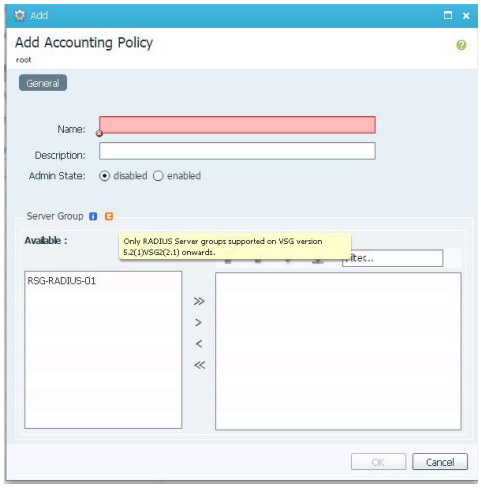
DETAILED STEPS

Step 1 Choose **Policy Management** > **Device Configurations** > **root** > **Policies** > **AAA** > **Accounting Policies**.

Step 2 In the General tab, click **Add Accounting Policy**.

Step 3 In the Add Accounting Policy dialog box, enter the information as described in following table, then click **OK**.

Figure 5: Add Accounting Policy Dialog Box



Add Accounting Policy Dialog Box

Field	Description
Name	Policy name.
Description	A brief policy description.
Admin State	Whether the administrative state of the policy is enabled or disabled.
Server Group	Select the server groups in "Available" Group and with the arrows buttons move them to "Assigned" Group. **Note** Ensure that the SSH Access Method is defined for all the selected server Groups.

Configuring Global Server Timers

Note Supported only by Compute Firewall in Cisco VSG Release 5.2.(1)VSG2(2.x) and later releases.

SUMMARY STEPS

1. Choose **Policy Management** > **Device Configurations** > **root** > **Policies** > **AAA** > **Remote Server Groups**.
2. In the General tab, click **Global Server Timers**.
3. In the Add Global Server Timers dialog box, enter the information as described in following table, then click **OK**.

DETAILED STEPS

Step 1 Choose **Policy Management** > **Device Configurations** > **root** > **Policies** > **AAA** > **Remote Server Groups**.

Step 2 In the General tab, click **Global Server Timers**.

Step 3 In the Add Global Server Timers dialog box, enter the information as described in following table, then click **OK**.

Add Global Server Timers Dialog Box

Field	Description
Name	Name of the Global Server Timer.
Description	A brief description of the timer.
Admin State	Whether the administrative state of the policy is enabled or disabled.
Dead Time	Duration for which non-reachable server is skipped.
Timeout	Server timeout period.
Retransmit Count	Retry count for server request.
Global Server Monitoring Parameters	
Idle Time	Time interval for monitoring the server.
User Name	Username in test packets for server monitoring only.
Password	Password for the User.

Configuring Core File Policies

Adding a Core File Policy for a Device

You can add a core file policy at any organizational level.

SUMMARY STEPS

1. Choose **Policy Management > Device Configurations > root > Policies > Core File**.
2. In the General tab, click **Add Core File Policy**.
3. In the Add Core File Policy dialog box, add the information as described in the following table, then click **OK**:

DETAILED STEPS

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Core File**.

Step 2 In the General tab, click **Add Core File Policy**.

Step 3 In the Add Core File Policy dialog box, add the information as described in the following table, then click **OK**:

Field	Description
Name	Core file policy name, containing 1 to 32 characters. You can use alphanumeric characters, hyphen (-), underscore (_), and period (.). You cannot change the name after the policy has been saved.
Description	Brief policy description, containing 1 to 256 characters. You can use alphanumeric characters, hyphen (-), underscore (_), and period (.).
Admin State	Indicate whether the administrative state of the policy is to be enabled or disabled.
Hostname/IP Address	Hostname or IP address to use for this policy. If you use a hostname rather than an IP address, you must configure a DNS server in .
Port	Port number for sending the core dump file.
Protocol	Protocol for exporting the core dump file (tftp only).
Path	Path to use when storing the core dump file on a remote system. The default path is /tftpboot; for example, /tftpboot/*test*, where *test* is the subfolder.

Editing a Core File Policy for a Device Profile

SUMMARY STEPS

1. Choose **Policy Management** > **Device Configurations** > **root** > **Policies** > **Core File**.
2. In the General tab, select the core file policy you want to edit, then click **Edit**.
3. In the Edit Core File Policy dialog box, edit the fields as required, using the information in the following table, then click **OK**.

DETAILED STEPS

Step 1 Choose **Policy Management** > **Device Configurations** > **root** > **Policies** > **Core File**.

Step 2 In the General tab, select the core file policy you want to edit, then click **Edit**.

Step 3 In the Edit Core File Policy dialog box, edit the fields as required, using the information in the following table, then click **OK**.

Field	Description
Name	Name of the core file policy (read-only).
Description	Brief policy description.
Admin State	Administrative status of the policy: enabled or disabled.
Hostname	Hostname or IP address. If you use a hostname, you must configure a DNS server.
Port	Port number to use when exporting the core dump file.
Protocol	Protocol used to export the core dump file (tftp only).
Path	Path to use when storing the core dump file on the remote system. The default path is /tftpboot. To specify a subfolder under tftpboot, use the format /tftpboot/*folder* where *folder* is the subfolder.

Deleting a Core File Policy from a Device Profile

SUMMARY STEPS

1. Choose **Policy Management > Device Configurations > root > Policies > Core File**.
2. In the General tab, select the core file policy you want to delete, then click **Delete**.
3. When prompted, confirm the deletion.

DETAILED STEPS

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Core File**.

Step 2 In the General tab, select the core file policy you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Configuring Fault Policies

Adding a Fault Policy for a Device Profile

You can add a fault policy at any organizational level.

SUMMARY STEPS

1. Choose **Policy Management** > **Device Configurations** > **root** > **Policies** > **Fault**.
2. In the General tab, click **Add Fault Policy**.
3. In the Add Fault Policy dialog box, enter the information as described in the following table, then click **OK**.

DETAILED STEPS

Step 1 Choose **Policy Management** > **Device Configurations** > **root** > **Policies** > **Fault**.

Step 2 In the General tab, click **Add Fault Policy**.

Step 3 In the Add Fault Policy dialog box, enter the information as described in the following table, then click **OK**.

Field	Description
Name	Fault policy name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, period, and colon. You cannot change this name after it is created.
Description	Brief policy description.
Flapping Interval	Length of time (in hours, minutes, and seconds) that must elapse before the system allows a fault to change its state. 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 default flapping interval is ten seconds.
Clear Faults Retention Action	Action to be taken when faults are cleared: • retain—Retain the cleared faults. • delete—Delete fault messages as soon as they are marked as cleared.

Field	Description
Clear Faults Retention Interval	How long the system is to retain cleared fault messages: • Forever—The system retains all cleared fault messages regardless of their age. • Other—The system retains cleared fault message for a specified the length of time. In the spinbox that is displayed when you select this option, enter the length of time (in days, hours, minutes, and seconds) that the system is to retain cleared fault messages.

Editing a Fault Policy for a Device Profile

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

SUMMARY STEPS

1. Choose **Policy Management > Device Configurations > root > Policies > Fault**.
2. In the General tab, select the fault policy you want to edit, then click **Edit**.
3. In the Edit Fault Policy dialog box, modify the following fields as required, then click **OK**.

DETAILED STEPS

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Fault**.

Step 2 In the General tab, select the fault policy you want to edit, then click **Edit**.

Step 3 In the Edit Fault Policy dialog box, modify the following fields as required, then click **OK**.

Field	Description
Name	Policy name (read-only).
Description	Brief policy description.

Field	Description
Flapping Interval	Length of time (in hours, minutes, and seconds) that must elapse before the system allows a fault to change its state. 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 recurs during the flapping interval, the fault returns to the active state. If the condition does not recur during the flapping interval, the fault is cleared. The next action depends on the setting in the Clear Faults Retention Action field. The default flapping interval is ten seconds.
Clear Faults Retention Action	Available fault retention actions: • retain—The system retains fault messages. • delete—The system deletes fault messages when they are marked as cleared.
Clear Faults Retention Interval	How long the system is to retain cleared fault messages: • Forever—The system retains all cleared fault messages regardless of their age. • Other—The system retains cleared fault message for a specified the length of time. In the spinbox that is displayed when you select this option, enter the length of time (in days, hours, minutes, and seconds) that the system is to retain cleared fault messages.

Deleting a Fault Policy for a Device Profile

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

SUMMARY STEPS

1. Choose **Policy Management > Device Configurations > root > Policies > Fault**.
2. In the General tab, select the fault policy that you want to delete, then click **Delete**.
3. When prompted, confirm the deletion.

DETAILED STEPS

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Fault**.

Step 2 In the General tab, select the fault policy that you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Configuring Log File Policies

Adding a Logging Policy for a Device Profile

You can add a logging policy for a device at any organizational level.

SUMMARY STEPS

1. Choose **Policy Management > Device Configurations > root > Policies > Log File**.
2. In the General tab, click **Add Logging Policy**.
3. In the Add Logging Policy dialog box, complete the following fields, then click **OK**.

DETAILED STEPS

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Log File**.

Step 2 In the General tab, click **Add Logging Policy**.

Step 3 In the Add Logging Policy dialog box, complete the following fields, then click **OK**.

Field	Description
Name	Logging policy name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, period, and colon. You cannot change this name after it is created.
Description	Brief policy description.

Field	Description
Log Level	One of the following logging severity levels: • debug0 • debug1 • debug2 • debug3 • debug4 • info • warning • minor • major • critical The default log level is info.
Backup Files Count	Number of backup files that are filled before they are overwritten. The range is 1 to 9 files, with a default of 2 files.
File Size (bytes)	Backup file size. The range is 1 MB to 100 MB with a default of 5 MB.

Editing a Logging Policy for a Device Profile

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

SUMMARY STEPS

1. Choose **Policy Management > Device Configurations > root > Policies > Log File**.
2. In the General tab, select the log file policy that you want to edit, then click **Edit**.
3. In the Edit Log File Policy dialog box, edit the fields as required by using the information in the following table, then click **OK**.

DETAILED STEPS

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Log File**.

Step 2 In the General tab, select the log file policy that you want to edit, then click **Edit**.

Step 3 In the Edit Log File Policy dialog box, edit the fields as required by using the information in the following table, then click **OK**.

Field	Description
Name	Logging policy name (read-only).
Description	Brief policy description.
Log Level	One of the following logging levels: • debug0 • debug1 • debug2 • debug3 • debug4 • info • warning • minor • major • critical The default log level is info.
Backup Files Count	Number of backup files that are filled before they are overwritten. The range is 1 to 9 files, with a default of 2 files.
File Size (bytes)	Backup file size. The range is 1 MB to 100 MB with a default of 5 MB.

Deleting a Logging Policy for a Device Profile

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

SUMMARY STEPS

1. Choose **Policy Management > Device Configurations > root > Policies > Log File**.
2. In the General tab, select the logging policy you want to delete, then click **Delete**.
3. When prompted, confirm the deletion.

DETAILED STEPS

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Log File**.
Step 2 In the General tab, select the logging policy you want to delete, then click **Delete**.
Step 3 When prompted, confirm the deletion.

Configuring SNMP Policies

Adding an SNMP Policy

You can add an SNMP policy at any organizational level.

SUMMARY STEPS

1. Choose **Policy Management** > **Device Configurations** > **root** > **Policies** > **SNMP**.
2. In the General tab, click **Add SNMP Policy**.
3. In the Add SNMP dialog box, complete the following fields as appropriate:
4. Click the **Configuration** tab, then complete the following steps:
5. In the Add SNMP dialog box, click **OK**.

DETAILED STEPS

Step 1 Choose **Policy Management** > **Device Configurations** > **root** > **Policies** > **SNMP**.
Step 2 In the General tab, click **Add SNMP Policy**.
Step 3 In the Add SNMP dialog box, complete the following fields as appropriate:

Table 6: General Tab

Field	Description
Name	SNMP policy name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, period, and colon. You cannot change this name after it is created.
Description	SNMP policy description. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, period, and colon.
Admin State	Indicate whether the administrative status of the policy is enabled or disabled.
Location	Physical location of the device.
Contact	Contact person for the device.
SNMP Port	Port that the SNMP agent listens to for requests. You cannot edit this field.

Step 4 Click the **Configuration** tab, then complete the following steps:

a) Click **Add SNMP User**.

b) In the **Add SNMP User** dialog box, complete the following fields as appropriate, then click **OK**:

Name	Description
User Name	SNMP v3 user name.
Authentication	
Policy Type	Choose a policy type: • md5 • sha
Password	Password for SNMP user.
Encryption	

Enable	Check this box to enable Encryption. In addition to authentication, provides DES 56-bit encryption based on the Cipher Block Chaining (CBC)-DES (DES-56) standard. Choosing this option means **authPriv** mode.
Use aes-128	Choosing *aes-128* token indicates that this privacy password is for generating a 128-bit AES key.
Privacy Password	Password to be associated with this privacy protocol.

c) Click **Add SNMP Community**.
d) In the **Add SNMP Community** dialog box, complete the following fields as appropriate, then click **OK**:

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

Step 5 In the Add SNMP dialog box, click **OK**.

Editing an SNMP Policy

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

SUMMARY STEPS

1. Choose **Policy Management > Device Configurations > root > Policies > SNMP**.
2. In the **General** tab, select the SNMP policy that you want to edit, then click **Edit**.
3. In the **Edit SNMP Policy** dialog box, edit the information in the General tab as required, using the information in the following table:
4. In the **Configuration** tab, edit the information as required:
5. In the Traps tab, edit the information as required:
6. Click **OK**.

DETAILED STEPS

Step 1 Choose **Policy Management > Device Configurations > root > Policies > SNMP**.

Step 2 In the **General** tab, select the SNMP policy that you want to edit, then click **Edit**.

Step 3 In the **Edit SNMP Policy** dialog box, edit the information in the General tab as required, using the information in the following table:

Field	Description
Name	SNMP policy name (read-only).
Description	Brief policy description.
Admin State	Administrative state of the policy: enabled (default) or disabled.
Location	Physical location of the device.
Contact	Contact person for the device.
SNMP Port	Port that the SNMP agent listens to for requests (read-only).

Step 4 In the **Configuration** tab, edit the information as required:

Field	Description
Add SNMP User	Adds an SNMP v3 User.
Add SNMP Community	Adds an SNMP community.
Delete	Select and delete the selected SNMP community or user.
Filter	Enter the string or value that you want to filter the table contents by.
Name	SNMP v3 User name.

Field	Description
Community	SNMP community name.
Role	Role associated with the SNMP community.

Step 5 In the Traps tab, edit the information as required:

Field	Description
Add SNMP Trap	Adds an SNMP trap.
Edit	Enables you to edit the selected SNMP trap.
Delete	Deletes the selected SNMP trap.
Filter	Enter the string or value that you want to filter the table contents by.
Hostname/IP Address	IP address of the SNMP host.
Port	Port where the SNMP agents listens for requests.
Community	SNMP community name.

Step 6 Click **OK**.

Deleting an SNMP Policy

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

SUMMARY STEPS

1. Choose **Policy Management > Device Configurations > root > Policies > SNMP**.
2. In the General tab, select the SNMP policy that you want to delete, then click **Delete**.
3. When prompted, confirm the deletion.

DETAILED STEPS

Step 1 Choose **Policy Management > Device Configurations > root > Policies > SNMP**.

Step 2 In the General tab, select the SNMP policy that you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Adding an SNMP Trap Receiver

SUMMARY STEPS

1. Choose **Policy Management** > **Device Configurations** > **root** > **Policies** > **SNMP**.
2. In the General tab, click **Add SNMP Policy** > **Traps** > **Add SNMP Trap**.
3. In the Add SNMP Trap dialog box, enter the following information, then click **OK**:

DETAILED STEPS

Step 1 Choose **Policy Management** > **Device Configurations** > **root** > **Policies** > **SNMP**.

Step 2 In the General tab, click **Add SNMP Policy** > **Traps** > **Add SNMP Trap**.

Step 3 In the Add SNMP Trap dialog box, enter the following information, then click **OK**:

Field	Description
Hostname/IP Address	Hostname or IP address of the SNMP host.
Port	Port that the SNMP agent listens to for requests. The default port is 162.
Community	SNMP community name.

Editing an SNMP Trap Receiver

SUMMARY STEPS

1. Choose **Policy Management > Device Configurations > root > Policies > SNMP**.
2. In the General tab, select the SNMP policy with the SNMP trap that you want to edit, then click **Edit**.
3. In the Edit SNMP Policy dialog box, click the **Traps** tab.
4. In the Traps tab, select the entry that you want to edit, then click **Edit**.
5. In the Edit SNMP Trap dialog box, edit the information in the General tab as required, using the following information:
6. Click **OK** in the open dialog boxes.

DETAILED STEPS

Step 1 Choose **Policy Management > Device Configurations > root > Policies > SNMP**.

Step 2 In the General tab, select the SNMP policy with the SNMP trap that you want to edit, then click **Edit**.

Step 3 In the Edit SNMP Policy dialog box, click the **Traps** tab.

Step 4 In the Traps tab, select the entry that you want to edit, then click **Edit**.

Step 5 In the Edit SNMP Trap dialog box, edit the information in the General tab as required, using the following information:

Field	Description
Hostname/IP Address	Hostname or IP address of the SNMP host (read-only).
Port	Port that the SNMP agent listens to for requests.
Community	SNMP community name.

Step 6 Click **OK** in the open dialog boxes.

Deleting an SNMP Trap Receiver

SUMMARY STEPS

1. Choose **Policy Management > Device Configurations > root > Policies > SNMP**.
2. In the General tab, select the SNMP policy with the SNMP trap that you want to delete, then click **Edit**.
3. In the Edit SNMP Policy dialog box, click the **Traps** tab.
4. In the Traps tab, select the entry that you want to delete, then click **Delete**.
5. When prompted, confirm the deletion.

DETAILED STEPS

Step 1 Choose **Policy Management > Device Configurations > root > Policies > SNMP**.
Step 2 In the General tab, select the SNMP policy with the SNMP trap that you want to delete, then click **Edit**.
Step 3 In the Edit SNMP Policy dialog box, click the **Traps** tab.
Step 4 In the Traps tab, select the entry that you want to delete, then click **Delete**.
Step 5 When prompted, confirm the deletion.

Configuring Syslog Policies

Adding a Syslog Policy for a Device

enables you to configure syslog policies for syslog messages and then attach a created syslog policy to a device profile for implementation on all devices using that profile.

You can create syslog policies for logging syslog messages to a remote syslog server or to a local buffer for later review.

SUMMARY STEPS

1. Choose **Policy Management > Device Configurations > root > Policies > Syslog**.
2. In the General tab, click **Add Syslog Policy**.
3. In the Add Syslog dialog box, provide the information as described in Add Syslog Policy Dialog Box, on page 173, then click **OK**.

DETAILED STEPS

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Syslog**.
Step 2 In the General tab, click **Add Syslog Policy**.
Step 3 In the Add Syslog dialog box, provide the information as described in Add Syslog Policy Dialog Box, on page 173, then click **OK**.

Field Descriptions

Add Syslog Policy Dialog Box

Field	Description
General Tab	
Name	Policy name.

Field	Description
Description	Brief policy description.
Use Emblem Format	Check the check box to use the EMBLEM format for syslog messages. This option appears only on supported devices.
Continue if Host is Down	Check the check box to continue logging if the syslog server is down. This option only appears on supported devices.
Servers Tab	
Add Syslog Server	Click to add a new syslog server.
Syslog Servers table	List of configured syslog servers.
Local Destinations Tab	
Console	• Admin State—Administrative state of the policy: disabled or enabled. • Level—Message level: alert, critical, or emergency. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency.
Monitor	• Admin State—Administrative state of the policy: disabled or enabled. • Level—Message level: emergency, alert, critical, error, warning, notification, information, or debugging. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency.

Field	Description
File	• Admin State—Administrative state of the policy: disabled or enabled. • Level—Message level: emergency, alert, critical, error, warning, notification, information, or debugging. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency. • File Name—Name of the file to which messages are logged. • Size (bytes)—Maximum size, in bytes, that the file can reach before the system begins to overwrite the messages.
Buffer	• Admin State—Administrative state of the policy: disabled or enabled. • Level—Message level: emergency, alert, critical, error, warning, notification, information, or debugging. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency. • Buffer Size (Bytes)—In bytes, the size of the buffer for syslog messages. • Wrap to Flash—Indicates whether or not the buffer contents are saved to flash memory when the buffer wraps (becomes full). Check the check box to save the contents to flash memory if the buffer wraps. • Max File Size in Flash (KB)—Maximum size, in kilobytes, that can be used by the syslog buffer. This option is enabled if the Wrap to Flash option is enabled. • Min Free Flash Size (KB)—Minimum size, in kilobytes, that is allocated for the syslog buffer. This option is enabled if the Wrap to Flash option is enabled.

Field	Description
Time Stamp	Check the check box for each of the following options that you want to enable for timestamp display: • Enable Timestamp • Include Year • Include Milliseconds • Show Time Zone • Use Local Time Zone

Editing a Syslog Policy for a Device Profile

enables you to edit existing syslog policies as described in this procedure.

SUMMARY STEPS

1. Choose **Policy Management** > **Device Configurations** > **root** > **Policies** > **Syslog**.
2. In the General tab, select the policy you want to edit, then click **Edit**.
3. In the Edit Syslog Policy dialog box, in the General tab, edit the information as required, using the following information:
4. In the Servers tab, click **Add Syslog Server** to add a new syslog server, or select an existing server and click **Edit** to edit it.
5. In the Local Destinations tab, edit the information as required, using the following information:
6. Click **OK**.

DETAILED STEPS

Step 1 Choose **Policy Management** > **Device Configurations** > **root** > **Policies** > **Syslog**.

Step 2 In the General tab, select the policy you want to edit, then click **Edit**.

Step 3 In the Edit Syslog Policy dialog box, in the General tab, edit the information as required, using the following information:

Field	Description
Name	Policy name (read-only).
Description	Brief policy description.
Use Emblem Format	Check the check box to use the EMBLEM format for syslog messages. This option is supported for ASA 1000Vs. It is not supported for VSGs.
Continue if Host is Down	Check the check box to continue logging if the syslog server is down. This option is supported for ASA 1000Vs. It is not supported for VSGs.

Step 4 In the Servers tab, click **Add Syslog Server** to add a new syslog server, or select an existing server and click **Edit** to edit it.

Step 5 In the Local Destinations tab, edit the information as required, using the following information:

Field	Description
Console	• Admin State—Administrative state of the policy: enabled or disabled. • Level—Message level: alerts, critical, or 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.
Monitor	• Admin State—Administrative state of the policy: enabled or disabled. • Level—Message level: alert, critical, emergency, error, warning, notification, information, or debugging. 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	• Admin State—Administrative state of the policy: enabled or disabled. • Level—Message level: alert, critical, emergency, error, warning, notification, information, or debugging. 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—Name of the file to which messages are logged. • Size (bytes)—Maximum size, in bytes, that the file can reach before the system begins to overwrite the messages.

Field	Description
Buffer	• Admin State—Administrative state of the policy: enabled or disabled. • Level—Message level: alert, critical, emergency, error, warning, notification, information, or debugging. 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. • Buffer Size (Bytes)—In bytes, the size of the buffer for syslog messages. • Wrap to Flash—Indicates whether or not the buffer contents are saved to flash memory with the buffer wraps (becomes full). Check the check box to save the contents to flash memory if the buffer wraps. • Max File Size in Flash (KB)—Maximum size, in kilobytes, that can be used by the syslog buffer. This option is enabled if the Wrap to Flash option is enabled. • Min Free Flash Size (KB)—Minimum size, in kilobytes, that is allocated for the syslog buffer. This option is enabled if the Wrap to Flash option is enabled.
Time Stamp	Check the check box for each of the following options that you want to enable for displaying timestamps: • Enable Timestamp • Include Year • Include Milliseconds • Show Time Zone • Use Local Time Zone

Step 6 Click **OK**.

Deleting a Syslog Policy for a Device Profile

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

SUMMARY STEPS

1. Choose **Policy Management > Device Configurations > root > Policies > Syslog**.
2. In the General tab, select the syslog policy that you want to delete, then click **Delete**.
3. When prompted, confirm the deletion.

DETAILED STEPS

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Syslog**.

Step 2 In the General tab, select the syslog policy that you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Adding a Syslog Server for a Device Profile

SUMMARY STEPS

1. Choose **Policy Management > Device Configurations > root > Policies > Syslog**.
2. In the General tab, click **Add Syslog Policy**.
3. In the Add Syslog Policy dialog box, click the **Servers** tab, then click **Add Syslog Server**.
4. In the Add Syslog Server dialog box, provide the information as described in Add Syslog Server Dialog Box, on page 180, then click **OK** in the open dialog boxes.

DETAILED STEPS

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Syslog**.

Step 2 In the General tab, click **Add Syslog Policy**.

Step 3 In the Add Syslog Policy dialog box, click the **Servers** tab, then click **Add Syslog Server**.

Step 4 In the Add Syslog Server dialog box, provide the information as described in Add Syslog Server Dialog Box, on page 180, then click **OK** in the open dialog boxes.

Field Descriptions

Add Syslog Server Dialog Box

Field	Description
Server Type	One of the following server types: • primary • secondary • tertiary
Hostname/IP Address	Hostname or IP address where the syslog file resides. If you use a hostname, you must configure a DNS server.
Severity	One of the following severity levels: • emergencies (0) • alerts (1) • critical (2) • errors (3) • warnings (4) • notifications (5) • information (6) • debugging (7)

Field	Description
Forwarding Facility	One of the following forwarding facilities: • auth • authpriv • cron • daemon • ftp • kernel • local0 • local1 • local2 • local3 • local4 • local5 • local6 • local7 • lpr • mail • news • syslog • user • uucp
Admin State	Administrative state of the server: disabled or enabled.
Port	Port to use to send data to the syslog server. The default port selection is 514 for UDP.
Protocol	Protocol to use: TCP or UDP (default).
Use Transport Layer Security	Check the check box to use Transport Layer Security. This option is available only for TCP.
Server Interface	Interface to use to access the syslog server.

Editing a Syslog Server for a Device Profile

SUMMARY STEPS

1. Choose **Policy Management > Device Configurations > root > Policies > Syslog**.
2. In the General tab, select the required syslog policy, then choose **Edit**.
3. In the Edit Syslog Policy dialog box, from the **Servers** tab, select the syslog server you want to edit, then click **Edit**
4. In the Edit Syslog Server dialog box, edit the fields as required, using the information in the following table.
5. Click **OK** in the open dialog boxes to save your changes.

DETAILED STEPS

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Syslog**.

Step 2 In the General tab, select the required syslog policy, then choose **Edit**.

Step 3 In the Edit Syslog Policy dialog box, from the **Servers** tab, select the syslog server you want to edit, then click **Edit**

Step 4 In the Edit Syslog Server dialog box, edit the fields as required, using the information in the following table.

Field	Description
Server Type	One of the following server types: primary, secondary, or tertiary (read-only).
Hostname/IP Address	Hostname or IP address where the syslog file resides.
Severity	One of the following severity levels: • emergencies (0) • alerts (1) • critical (2) • errors (3) • warnings (4) • notifications (5) • information (6) • debugging (7)

Field	Description
Forwarding Facility	One of the following forwarding facilities: • auth • authpriv • cron • daemon • ftp • kernel • local0 • local1 • local2 • local3 • local4 • local5 • local6 • local7 • lpr • mail • news • syslog • user • uucp
Admin State	Administrative state of the policy: enabled or disabled.
Port	Port to use to send data to the syslog server. Valid port values are 1025 through 65535 for both TCP and UDP. The default TCP port is 1470. The default UDP port is 514.
Protocol	Protocol to use: TCP or UDP.
Use Transport Layer Security	Check the check box to use Transport Layer Security. This option is available only for TCP.

Field	Description
Server Interface	Interface to use to access the syslog server. This option applies to ASA 1000V only. Enter the data interface name specify in the edge firewall. Use the device CLI to configure a route through the management interface.

Step 5 Click **OK** in the open dialog boxes to save your changes.

Deleting a Syslog Server for a Device Profile

SUMMARY STEPS

1. Choose **Policy Management > Device Configurations > root > Policies > Syslog**.
2. In the General tab, select the syslog policy with the server you want to delete, then click **Edit**.
3. In the Edit Syslog Policy dialog box, click the **Servers** tab.
4. In the Servers tab, select the syslog server that you want to delete, then click **Delete**.
5. When prompted, confirm the deletion.
6. Click **OK** to save the policy.

DETAILED STEPS

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Syslog**.
Step 2 In the General tab, select the syslog policy with the server you want to delete, then click **Edit**.
Step 3 In the Edit Syslog Policy dialog box, click the **Servers** tab.
Step 4 In the Servers tab, select the syslog server that you want to delete, then click **Delete**.
Step 5 When prompted, confirm the deletion.
Step 6 Click **OK** to save the policy.

Configuring Device Profiles

Adding a Firewall Device Profile

SUMMARY STEPS

1. Choose **Policy Management** > **Device Configurations** > **root** > **Device Profiles**.
2. In the General tab, click **Add Device Profile**.
3. In the New Device Profile dialog box, enter the required information in the General and Policies tabs, then click **OK**:

DETAILED STEPS

Step 1 Choose **Policy Management** > **Device Configurations** > **root** > **Device Profiles**.

Step 2 In the General tab, click **Add Device Profile**.

Step 3 In the New Device Profile dialog box, enter the required information in the General and Policies tabs, then click **OK**:

Field	Description
DNS Servers	You can: • Add a new server. • Select an existing server and edit or delete it. • Use the arrows to change priority.
DNS Domains	You can: • Add a new domain. • Select an existing domain and edit or delete it.
NTP Servers	You can: • Add a new server. • Select an existing server and edit or delete it. • Use the arrows to change priority.
SNMP	You can: • Choose a policy from the drop-down list. • Add a new policy. • Click the Resolved Policy link to review or modify the policy currently assigned.

Field	Description
Syslog	You can: • Choose a policy from the drop-down list. • Add a new policy. • Click the Resolved Policy link to review or modify the policy currently assigned.
Fault	You can: • Choose a policy from the drop-down list. • Add a new policy. • Click the Resolved Policy link to review or modify the policy currently assigned.
Core File	You can: • Choose a policy from the drop-down list. • Add a new policy. • Click the Resolved Policy link to review or modify the policy currently assigned.
Policy Agent Log File	You can: • Choose a policy from the drop-down list. • Add a new policy. • Click the Resolved Policy link to review or modify the policy currently assigned.
Policy Engine Logging	Select the appropriate radio button to enable or disable logging.
Auth Policy	You can: • Choose a policy from the drop-down list. • Add a new policy. • Click the Resolved Policy link to review or modify the policy currently assigned.

Editing a Firewall Device Profile

After you create a firewall device profile, you can edit it as needed.

SUMMARY STEPS

1. Choose **Policy Management** > **Device Configurations** > **root** > **Device Profiles**.
2. In the Device Profiles pane, select the profile you want to edit, then click **Edit**.
3. In the Edit Firewall Device Policy dialog box, update the information in the General tab as described in the following table:
4. In the Policies tab, update the information as described in the following table, then click **OK**:

DETAILED STEPS

Step 1 Choose **Policy Management** > **Device Configurations** > **root** > **Device Profiles**.

Step 2 In the Device Profiles pane, select the profile you want to edit, then click **Edit**.

Step 3 In the Edit Firewall Device Policy dialog box, update the information in the General tab as described in the following table:

Field	Description
Name	Profile name. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, period, and colon. You cannot change this name after it is saved.
Description	Brief profile description. The description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphen, underscore, period, and colon.
Time Zone	Select the required time zone from the drop-down list.

Step 4 In the Policies tab, update the information as described in the following table, then click **OK**:

Field	Description
DNS Servers	
Add DNS Server	Adds a DNS server.
Edit	Enables you to edit the selected DNS server.
Delete	Deletes the selected DNS server.
Up and down arrows	Change the priority of the selected DNS server. uses the DNS servers in the order in which they appear in the table.
DNS Servers Table	
IP Address	IP addresses for the DNS servers configured in the system.

Field	Description
Server Interface	Interface to use to access the DNS server.
NTP Servers	
Add NTP Server	Click to add an NTP server.
Edit	Enables you to edit the selected NTP server.
Delete	Deletes the selected NTP server.
Up and down arrows	Change the priority of the selected NTP Server hostname. uses the NTP servers in the order in which they appear in the table.
NTP Servers Table	
Hostname / IP Address	NTP server name or IP address. For PNSC and VSG, enter either a hostname or IP address. If you are providing hostname, make sure to provide a valid DNS server. One NTP server entry is a must for VSG. For ASA 1000Vs, you must enter an IP address.
Interface Name	Interface to use to access the NTP server.
DNS Domains	
Add	Click to add a DNS domain name.
Edit	Click to edit the DNS domain name selected in the DNS Domains table. The default DNS name cannot be edited.
Delete	Click to delete the DNS domain name selected in the DNS Domains table.
DNS Domains table	Default DNS domain name and domain in the system.
Other Options	
SNMP	Select, add, or edit SNMP policies as needed.
Syslog	Select, add, or edit syslog policies as needed.
Fault	Select, add, or edit fault policies as needed.
Core File	Select, add, or edit core file policies as needed.
Policy Agent Log File	Select, add, or edit the policy agent log file policies as needed.

Field	Description
Policy Engine Logging	Select the appropriate radio button to enable or disable logging.
Auth Policy	Select an available authentication policy, or click **Add Auth Policy** to add a new authentication policy.

Deleting a Firewall Device Profile

SUMMARY STEPS

1. Choose **Policy Management > Device Configurations > root** > **Device Profiles**.
2. In the **Work** pane, click the device profile you want to delete.
3. Click **Delete.**
4. In the Confirm dialog box, click **OK**.

DETAILED STEPS

Step 1 Choose **Policy Management > Device Configurations > root** > **Device Profiles**.

Step 2 In the **Work** pane, click the device profile you want to delete.

Step 3 Click **Delete.**

Step 4 In the Confirm dialog box, click **OK**.

Configuring NTP

Network Time Protocol (NTP) is a networking protocol used to synchronize the time on a network of machines. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server.

enables you to configure NTP for compute firewalls, edge firewalls, and itself.

Configuring NTP for a compute or edge firewall requires the following steps:

1 Configuring a device profile with NTP.

2 Applying the device profile to a compute or edge firewall

The following topics describe how to perform these steps.

For information on configuring NTP on , see Adding an NTP Server, on page 62.

Creating a Device Profile with NTP

This procedure describes how to create a device profile with NTP that you can apply to an edge or compute firewall.

SUMMARY STEPS

1. Choose **Policy Management > Device Configurations > root > Device Profiles**.
2. In the General tab, click **Add Device Profile**.
3. In the New Device Profile dialog box, provide the following information:
4. Click the **Policies** tab.
5. In the NTP servers area, click **Add NTP Server**.
6. In the Add NTP Server dialog box, enter the information as described in Add NTP Server Dialog Box, on page 191, then click **OK**.
7. Click **OK**.

DETAILED STEPS

Step 1 Choose **Policy Management > Device Configurations > root > Device Profiles**.

Step 2 In the General tab, click **Add Device Profile**.

Step 3 In the New Device Profile dialog box, provide the following information:

- Name—Profile name.
- Description—Brief profile description.
- Time Zone—From the drop-down list, choose the time zone.

Step 4 Click the **Policies** tab.

Step 5 In the NTP servers area, click **Add NTP Server**.

Step 6 In the Add NTP Server dialog box, enter the information as described in Add NTP Server Dialog Box, on page 191, then click **OK**.

Step 7 Click **OK**.

What to Do Next

After you have configured the device profile, you can apply it to a firewall as described in the following topics:

- Applying Device Profiles to Edge Firewalls, on page 192
- Applying Device Profiles to Compute Firewalls, on page 191

Field Descriptions

Add NTP Server Dialog Box

Add NTP Server Dialog Box

Field	Description
Hostname/IP Address	NTP server name or IP address. For and VSGs, you can enter either a hostname or IP address. For ASA 1000Vs, you must enter an IP address. **Note** Starting with Cisco PNSC, Release 3.4.2, ensure that there is at least one NTP server entry for each Compute Firewall. If you enter host name for NTP server, you should also define a DNS server.
Interface Name	(Policy Management Device Profiles only) Device interface to reach the NTP server. Only ASA 1000Vs support interface names. • If you specify an interface, use the interface name specified by the edge firewall. • To use the management interface, you must configure the route by using the CLI.
Authentication Key	(Policy Management Device Profiles only) Authentication key to access the NTP server. Only ASA 1000Vs support authentication keys.

Applying Device Profiles to Compute Firewalls

After you have created a device profile, you can apply the profile to a compute firewall.

Note Starting with Cisco VSG Release 5.2.(1)VSG2(2.0), ensure that at least one NTP server is defined in Device Profile for Compute firewall.

SUMMARY STEPS

1. Choose **Resource Management > Managed Resources > root >** *tenant* **> Compute Firewalls >** *compute-firewall*.
2. In the General tab, click **Select** in the Device Profile field.
3. In the Select Device Profile dialog box, select the desired profile, then click **OK**.
4. Click **Save**.

DETAILED STEPS

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant* **> Compute Firewalls >** *compute-firewall*.
Step 2 In the General tab, click **Select** in the Device Profile field.
Step 3 In the Select Device Profile dialog box, select the desired profile, then click **OK**.
Step 4 Click **Save**.

Applying Device Profiles to Edge Firewalls

After you have created a device profile, you can apply the profile to an edge firewall.

SUMMARY STEPS

1. Choose **Resource Management > Managed Resources > root >** *tenant* **> Edge Firewalls >** *edge-firewall*.
2. In the General tab, click **Select** in the Device Profile field.
3. In the Select Device Profile dialog box, select the desired profile, then click **OK**.
4. Click **Save**.

DETAILED STEPS

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant* **> Edge Firewalls >** *edge-firewall*.
Step 2 In the General tab, click **Select** in the Device Profile field.
Step 3 In the Select Device Profile dialog box, select the desired profile, then click **OK**.
Step 4 Click **Save**.

Associating Device Policies with Profiles

After you create a device policy, you can associate it with a device profile. By doing so, you can ensure that all devices associated with the device profile use the same policy.

SUMMARY STEPS

1. Choose **Policy Management > Device Configurations > root > Device Profiles >** *profile* where *profile* is the device profile that you want to add the device policy to.
2. Click the **Policies** tab.
3. In the Policies tab, locate the drop-down list for the type of policy you want to associate, such as Syslog or Auth Policy.
4. From the drop-down list, choose the policy to add to the profile, then click **Save**.

DETAILED STEPS

Step 1 Choose **Policy Management > Device Configurations > root > Device Profiles >** *profile* where *profile* is the device profile that you want to add the device policy to.

Step 2 Click the **Policies** tab.

Step 3 In the Policies tab, locate the drop-down list for the type of policy you want to associate, such as Syslog or Auth Policy.

Step 4 From the drop-down list, choose the policy to add to the profile, then click **Save**.
The policy is automatically applied to all devices using the selected profile.

CHAPTER 11

Configuring Managed Resources

This section contains the following topics:

- Resource Management, page 195
- Registering Third-Party VMs in VMware, page 196
- Importing Service Images, page 200
- Compute Firewalls, page 201
- Edge Firewalls, page 207
- Edge Routers, page 211
- Load Balancers, page 216
- Adding a Port Profile to a VSM, page 222
- Updating Discovered VSM Port Profiles, page 223
- Troubleshooting Devices and Services, page 224
- Launching ASDM, page 224
- Managing VSG Pools, page 226

Resource Management

enables you to manage the following resources:

- Compute firewalls—A virtual firewall that delivers security and compliance for a virtual computing environment at the VM level. Context-based and VLAN-independent policies can be applied to VM zones, thereby providing topology-invariant, policy-based security controls. In addition, traffic from external sources to VMs, and from VM to VM can be protected.
- Edge firewalls—A virtual appliance that secures the tenant edge in a multitenant environment. An example of an edge firewall is a Cisco Adaptive Security Appliance 1000V (ASA 1000V). An edge firewall:
  - Supports site-to-site VPN, NAT, and DHCP.

- Acts as a default gateway.
- Secures the VMs within a tenant against network-based attacks.

- Edge routers—A virtual edge router that serves as a single-tenant WAN gateway in a multitenant cloud. It allows enterprises to extend their WANs into external provider-hosted clouds.
- Load balancers—A virtual appliance that distributes network and application traffic across multiple servers. It improves application performance and prevents server failures by alleviating loads on servers.
- Virtual Security Gateways (VSGs)—VSGs evaluate policies based on network traffic. The main functions of a VSG are as follows:
  - Receive traffic from Virtual Network Service Data Path (vPath). For every new flow, the vPath component encapsulates the first packet and sends it to a VSG as specified in the Nexus 1000V port profiles. It assumes that the VSG is Layer 2 adjacent to vPath. The mechanism used for communication between vPath and the VSG is similar to VEM and Nexus 1000V communication on a packet VLAN.
  - Perform application fix-up processing such as FTP, TFTP, and RSH.
  - Evaluate policies by inspecting the packets sent by vPath using network, VM, and custom attributes.
  - Transmit the policy evaluation results to vPath.

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

- Virtual Supervisor Modules (VSMs)—A virtual appliance that runs on a Nexus 1000V switch and that manages, monitors, and configures multiple Virtual Ethernet Modules (VEMs). VEMs run as part of a hypervisor where they act as virtual switches. VSMs are tightly integrated with hypervisors, so that configurations made on a VSM are automatically propagated to the VEMs. As a result, instead of configuring soft switches inside the hypervisor on a host-by-host basis, you can define configurations for immediate use on all VEMs that are managed by the VSM from a single interface.

Resource Management Configuration Workflow

You manage resources by placing them in service. The general workflow for placing devices in service is as follows:

1. Create tenants and subordinate organizations.
2. Configure device policies.
3. Register or instantiate service devices from service images.

Registering Third-Party VMs in VMware

To register third-party VMs in Prime Network Services Controller, install the Prime Network Services Controller Device Adapter before deploying and registering the third-party VMs.

Deploying the Prime Network Services Controller Device Adapter on VMware

The Prime Network Services Controller Device Adapter enables third-party VMs (such as Citrix NetScaler load balancers) to register with Prime Network Services Controller.

This procedure installs the Prime Network Services Controller Device Adapter on a VMware host using an OVA image. For information on how to deploy a VM using an ISO image, see the VMware documentation.

The following guidelines apply when deploying the Prime Network Services Controller Device Adapter:

- Prime Network Services Controller Device Adapter must be installed before you can deploy and register third-party service nodes, such as Citrix NetScaler load balancers.
- Adding or editing policies from the Prime Network Services Controller Device Adapter is not supported. All configuration must be performed using the Prime Network Services Controller GUI.
- You need to install the Prime Network Services Controller Device Adapter only once for each Prime Network Services Controller instance.
- If you reinitialize Prime Network Services Controller, you must also reinitialize Prime Network Services Controller Device Adapter.

Before You Begin

Confirm that a network path exists between the Prime Network Services Controller Device Adapter IP address and the Prime Network Services Controller management IP address.

SUMMARY STEPS

1. Use the VMware vSphere Client to log in to the vCenter server.
2. Choose the host on which to deploy the Prime Network Services Controller Device Adapter.
3. Choose **File > Deploy OVF Template**.
4. In the wizard, provide the required information as described in the following table:
5. Click **Finish**.
6. After the deployment is complete, power up the VM.
7. Confirm that the Prime Network Services Controller Device Adapter VM is successfully registered with Prime Network Services Controller by logging in to the Prime Network Services Controller server and choosing **Administration > Service Registry > Providers**.

DETAILED STEPS

Step 1 Use the VMware vSphere Client to log in to the vCenter server.

Step 2 Choose the host on which to deploy the Prime Network Services Controller Device Adapter.

Step 3 Choose **File > Deploy OVF Template**.

Step 4 In the wizard, provide the required information as described in the following table:

Screen	Action
Source	Navigate to and choose the file.

Screen	Action
OVF Template Details	Review the details of the Prime Network Services Controller Device Adapter template.
End User License Agreement	Review the agreement and click **Accept**.
Name and Location	Specify a name and location for the VM. The name must begin with a letter.
Storage	Choose the data store for the VM.
Disk Format	Choose the required format.
Network Mapping	Choose the management network port group for the VM.
Properties	Provide the following information: • VM IP address, subnet mask, and gateway IP address. • DNS server and NTP server IP addresses. • IP address for the Prime Network Services Controller server. • Password and shared secret password for access to the VM.
Ready to Complete	Review the deployment settings for accuracy.

Step 5 Click **Finish**.

Step 6 After the deployment is complete, power up the VM.
You can monitor the progress of the deployment by opening the VM console.

Step 7 Confirm that the Prime Network Services Controller Device Adapter VM is successfully registered with Prime Network Services Controller by logging in to the Prime Network Services Controller server and choosing **Administration > Service Registry > Providers**.
The Providers table should include managed-endpoint and mgmt-controller entries for the Prime Network Services Controller Device Adapter VM that you deployed.

Deploying a Citrix NetScaler Load Balancer on VMware

This procedure describes how to deploy third-party VMs (such as Citrix NetScaler load balancers) in VMware so that you can register them with Prime Network Services Controller.

Before You Begin

Confirm the following:

- Prime Network Services Controller Device Adapter is successfully registered with Prime Network Services Controller by choosing **Administration > Service Registry > Providers**. The Providers table

should include managed-endpoint and mgmt-controller entries for the Prime Network Services Controller Device Adapter VM.

- The third-party OVA is accessible from the VMware vSphere Client.

Note If you are prompted with a third-party login screen requesting information (for example, management IP information or upload feature licenses), you can do either of the following:

- Use the existing configuration and ignore this screen.
- Refer to the following URL for additional Citrix licensing features: http://support.citrix.com/proddocs/topic/netscaler-getting-started-map-10-1/ns-initial-config-using-ftu-wizard-tsk.html

SUMMARY STEPS

1. In VMware, choose the host on which to deploy the third-party VM.
2. Choose **File > Deploy OVF Template**.
3. In the wizard, provide the information described in the following table. The same information is required for both Citrix NetScaler 1000V and Citrix NetScaler VPX VMs.
4. In the Ready to Complete screen, review the deployment settings for accuracy, and then click **Finish**.
5. Open the VM console so that you can monitor the deployment status.
6. When prompted in the console, enter the following information for the VM:
7. When the information is correct, enter **4** and press **Return**.

DETAILED STEPS

Step 1 In VMware, choose the host on which to deploy the third-party VM.

Step 2 Choose **File > Deploy OVF Template**.

Step 3 In the wizard, provide the information described in the following table. The same information is required for both Citrix NetScaler 1000V and Citrix NetScaler VPX VMs.

Screen	Action
Source	Choose the OVA that you want to deploy.
OVF Template Details	Review the details.
Name and Location	Enter a name and choose a location for the VM.
Storage	Choose the location for the VM files.
Disk Format	Choose the format in which to store the virtual disks.
Network Mapping	Choose the destination networks for the VM.

Step 4 In the Ready to Complete screen, review the deployment settings for accuracy, and then click **Finish**.

Step 5 Open the VM console so that you can monitor the deployment status.

Step 6 When prompted in the console, enter the following information for the VM:

- IP address
- Subnet mask
- Gateway IP address

Step 7 When the information is correct, enter **4** and press **Return**.
You can monitor the deployment progress in the console.
After the VM is deployed, you can register it in Prime Network Services Controller.

Verifying VM Registration

Use this procedure to verify that the following VMs are successfully registered in :

- ASA 1000V
- CSR 1000V
- InterCloud
- Citrix NetScaler load balancer
- VSG
- VSM

To confirm registration with , choose **Resource Management > Resources >** *resource*. In the content pane, the consolidated status for each resource is displayed in the Status column. This consolidated status is determined by assessing the following attributes in sequence:

1. Reachability
2. Association
3. Config State
4. Running

If any of these attributes fail, the failure of that attribute is displayed. For example, if the device cannot be reached, the status *unreachable* is displayed. Similarly, if the device is reachable and associated, but the configuration fails, the status *config failed* is displayed.

Importing Service Images

enables you to import service images that you can then use to instantiate a device or service VM.

After you import an image, automatically places the file in the correct location and populates the Images table.

Before You Begin

Confirm that the service images are available for importing into .

Step 1 Choose **Resource Management > Resources > Images**.

Step 2 Click **Import Service Image**.

Step 3 In the Importing Service Image Dialog box:

a) Enter a name and description for the image you are importing.
b) In the Type field, choose the type of image to import.
c) In the Version field, enter a version number that you want to assign to the image.
d) In the Import area, provide the following information, and then click **OK**:

- Protocol to use for the import operations: FTP, SCP, or SFTP.
- Hostname or IP address of the remote host with the images.
- Account username and password for the remote host.
- Absolute image path and filename, starting with a slash (/).

Compute Firewalls

Adding a Compute Firewall

You can add a compute firewall and assign it to a VSG, thereby placing the VSG in service. A wizard walks you through the configuration process, which includes assigning profiles, assigning a VSG or instantiating a VSG service image, and configuring interfaces.

When you add a new compute firewall, the firewall data IP address can be the same as the data IP address of an existing compute firewall in as long as the firewalls have different organizational paths. That is, as long as the firewalls do not reside in the same organization, including parent and child organizations.

Note We recommend that you add the compute firewall at the tenant level or below, and not at the root level.

SUMMARY STEPS

1. Choose **Resource Management > Managed Resources > root >** *tenant*.
2. In the Network Services tab, choose **Add Compute Firewall**.
3. In the Properties screen, provide the information as described in Properties Screen, on page 203, and then click **Next**.
4. In the Service Device screen, select the required VSG service device, provide any required information as described in Service Device Screen, on page 204, and then click **Next**.
5. (Instantiate option only) If you instantiate a VSG service device from an image, do one or both of the following in the Placement screen, and then click **Next**:
   - Navigate to and choose the host or resource pool to use for the VSG instance.
   - If you enabled high availability, either check the **Same as Primary** check box, or navigate to and choose the host or resource pool to use for the secondary VSG instance.
6. In the Interfaces screen, configure interfaces as follows, and then click **Next**:
   - If you assigned a VSG, enter the data IP address and subnet mask.
   - If you assigned a VSG pool, enter the data IP address and subnet mask.
   - If you instantiated a VSG service device without high availability, add management and data interfaces.
   - If you instantiated a VSG service device with high availability, add management, data, and HA interfaces.
7. In the Summary screen, confirm that the information is correct, and then click **Finish**.

DETAILED STEPS

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant*.

Step 2 In the Network Services tab, choose **Add Compute Firewall**.

Step 3 In the Properties screen, provide the information as described in Properties Screen, on page 203, and then click **Next**.

Step 4 In the Service Device screen, select the required VSG service device, provide any required information as described in Service Device Screen, on page 204, and then click **Next**.

Step 5 (Instantiate option only) If you instantiate a VSG service device from an image, do one or both of the following in the Placement screen, and then click **Next**:

- Navigate to and choose the host or resource pool to use for the VSG instance.
- If you enabled high availability, either check the **Same as Primary** check box, or navigate to and choose the host or resource pool to use for the secondary VSG instance.

Step 6 In the Interfaces screen, configure interfaces as follows, and then click **Next**:

- If you assigned a VSG, enter the data IP address and subnet mask.
- If you assigned a VSG pool, enter the data IP address and subnet mask.
- If you instantiated a VSG service device without high availability, add management and data interfaces.

- If you instantiated a VSG service device with high availability, add management, data, and HA interfaces.

For field-level help when configuring the interfaces, see the online help.

Step 7 In the Summary screen, confirm that the information is correct, and then click **Finish**.

Compute Firewall Deployment Options

VSG compute firewalls are available in the following deployment models based on the memory, CPU speed, and number of virtual CPUs. Choose the deployment size that is appropriate for your environment.

Deployment Size	Memory	CPU Speed	Number of Virtual CPUs
Small	2 GB	1.0 GHz	1
Medium	2 GB	1.5 GHz	1
Large	2 GB	1.5 GHz	2

Field Descriptions

Properties Screen

Field	Description
Name	Compute firewall name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, period, and colon. You cannot change this name after it is created.
Description	Compute firewall description.
Host Name	Management hostname of the firewall.
Device Profile	Do either of the following: • Click the profile name to view or optionally modify the currently assigned device configuration profile. • Click **Select** to choose a different device configuration profile.

Service Device Screen

Field	Description
Assign VSG	Assign a VSG to the compute firewall. From the **VSG Device** drop-down list, choose the required service device.
Assign VSG Pool	Assign a VSG pool to the compute firewall. In the **VSG Pool** field, either choose the required pool from the drop-down list or click **Add Pool** to add a new pool.
Instantiate	Instantiate a VSG service device from an available image. **1** In the list of available images, select the image to use to instantiate a new VSG service device. **2** In the High Availability field, check the **Enable HA** check box to enable high availability. **3** From the Deployment Size drop-down list, choose the size of the deployment. For more information, see Compute Firewall Deployment Options, on page 203. **4** In the VM Access password fields, enter the password for the admin user account.

Managing Compute Firewalls

You can edit and view fault information on existing compute firewalls as needed.

SUMMARY STEPS

1. In the Resource Management tab, choose **Managed Resources > root >** *tenant*.
2. In the Network Services tab, select the required compute firewall, and then select an operation to perform.
3. If you chose **Edit**, modify the fields as appropriate, using the information in the following tables, and then click **OK**.

DETAILED STEPS

Step 1 In the Resource Management tab, choose **Managed Resources > root >** *tenant*.

Step 2 In the Network Services tab, select the required compute firewall, and then select an operation to perform.

Step 3 If you chose **Edit**, modify the fields as appropriate, using the information in the following tables, and then click **OK**.

Note To view additional information about an entry in the Faults tab, double-click the entry, or select the entry and then click **Properties**.

General Tab

Field	Description
Name	Compute firewall name.
Description	Compute firewall description.
Management IP Address	Management IP address for the compute firewall.
HA Role	High availability role of the compute firewall: standalone or active standby.
Deployment Size	Size of the deployment: Small, Medium, or Large.
Device Profile	Device profile associated with the compute firewall.
Status	
Deploy State	Deployment state of the firewall.
Power State	Whether the firewall is powered off or on.
Config Status	Configuration status of the compute firewall: applied, applying, failed-to-apply, or not-applied.
Association Status	Association state of the firewall: associated, associating, disassociating, failed, or unassociated.
Reachable	Whether or not the compute firewall is reachable.

Placement Tab

This tab is displayed only if the compute firewall is instantiated from a service image.

Field	Description
Image Table (read-only)	
Select	Radio-button indicating image selection.
Image name	Service image name.
Version	Service image version.
VM Manager Details If high availability is enabled, the following fields are displayed for both the primary and secondary service devices.	
VM Manager	VM Manager for the service device.
Host	IP address of the VM host.

Field	Description
Instance Name	VM instance name.

Network Interfaces Tab—VSG Assigned

This tab is displayed only if a VSG was assigned to the compute firewall.

Field	Description
Management Hostname	Management hostname for the compute firewall.
Data IP Address	Compute firewall data IP address.
Data IP Subnet	Netmask for the data IP address.
VLAN	VLAN to use for service path configuration if the device is running in Layer 2 mode.

Network Interfaces Tab—VSG Instantiated

This tab is displayed only if the compute firewall was instantiated from a service image.

Field	Description
Toolbar	
Add Interface	Adds an interface.
Edit	Enables you to edit the selected interface.
Delete	Deletes the selected interface.
Filter	Filters the table contents by the string or value that you enter.
Table	
Type	Interface type: Data, HA, or Management.
IP Address	Interface IP address.
Port Group / Sub Network	Port group or subnetwork associated with the interface.

Unassigning a VSG

Use this procedure to remove a VSG from a compute firewall.

SUMMARY STEPS

1. Choose **Resource Management > Managed Resources > root >** *tenant*.
2. In the Network Services tab, choose the compute firewall with the VSG that you want to unassign.
3. In the toolbar, choose **Actions > Unassign VSG**.
4. When prompted, confirm the action.

DETAILED STEPS

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant*.

Step 2 In the Network Services tab, choose the compute firewall with the VSG that you want to unassign.

Step 3 In the toolbar, choose **Actions > Unassign VSG**.

Step 4 When prompted, confirm the action.

Edge Firewalls

Adding an Edge Firewall

You can add an edge firewall and assign it to an ASA 1000V, thereby placing the ASA 1000V in service. A wizard walks you through the configuration process, which includes assigning configuration and service profiles, assigning an ASA 1000V or instantiating an ASA 1000V service image, and configuring interfaces.

Before You Begin

- At least one of the following must exist:
  - An ASA 1000V must be registered in Prime Network Services Controller and must be available for assignment.
  - An imported ASA 1000V service image.
- A VM Manager must be configured in Prime Network Services Controller.

SUMMARY STEPS

1. Choose **Resource Management > Managed Resources > root >** *tenant*.
2. In the Network Services tab, choose **Add Edge Firewall**.
3. In the Properties screen, provide the information described in Properties Screen, on page 210, and then click **Next**.
4. In the Service Device screen, do one of the following, and then click **Next**:
   - To assign an existing ASA 1000V service device:
     1. Click **Assign ASA 1000V**.
     2. From the **ASA 1000V Device** drop-down list, choose the required ASA 1000V.
   - To instantiate a new ASA 1000V:
     1. Click **Instantiate**.
     2. Choose the image to use to instantiate a new ASA 1000V service device.
     3. In the VM Access password fields, enter the password for the admin user account.
5. (Instantiate option only) If you instantiate a ASA 1000V service device from an image, do one or both of the following in the Placement screen, and then click **Next**:
   - Navigate to and choose the host or resource pool to use for the ASA 1000V instance.
   - If you enabled high availability, either check the **Same as Primary** check box, or navigate to and choose the host or resource pool to use for the secondary ASA 1000V instance.
6. In the Interfaces screen, add the required interfaces as follows, and then click **Next**:
   - If you assigned an ASA 1000V without high availability, configure one inside and one outside interface.
   - If you assigned an ASA 1000V with high availability, configure one inside and one outside interface, each with a secondary IP address.
   - If you instantiated an ASA 1000V without high availability, configure management, inside, and outside interfaces.
   - If you instantiated an ASA 1000V with high availability, configure management, inside, outside, and HA interfaces.

     Note The management and HA interfaces must use different port profiles.
7. In the Summary screen, confirm that the information is accurate, and then click **Finish**.
8. If you instantiated the ASA 1000V from a service image, you must do the following to ensure registration with Prime Network Services Controller:

DETAILED STEPS

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant*.

Step 2 In the Network Services tab, choose **Add Edge Firewall**.

Step 3 In the Properties screen, provide the information described in Properties Screen, on page 210, and then click **Next**.

Step 4 In the Service Device screen, do one of the following, and then click **Next**:

- To assign an existing ASA 1000V service device:
  1. Click **Assign ASA 1000V**.
  2. From the **ASA 1000V Device** drop-down list, choose the required ASA 1000V.
- To instantiate a new ASA 1000V:
  1. Click **Instantiate**.
  2. Choose the image to use to instantiate a new ASA 1000V service device.
  3. In the VM Access password fields, enter the password for the admin user account.

Step 5 (Instantiate option only) If you instantiate a ASA 1000V service device from an image, do one or both of the following in the Placement screen, and then click **Next**:

- Navigate to and choose the host or resource pool to use for the ASA 1000V instance.
- If you enabled high availability, either check the **Same as Primary** check box, or navigate to and choose the host or resource pool to use for the secondary ASA 1000V instance.

Step 6 In the Interfaces screen, add the required interfaces as follows, and then click **Next**:

- If you assigned an ASA 1000V without high availability, configure one inside and one outside interface.
- If you assigned an ASA 1000V with high availability, configure one inside and one outside interface, each with a secondary IP address.
- If you instantiated an ASA 1000V without high availability, configure management, inside, and outside interfaces.
- If you instantiated an ASA 1000V with high availability, configure management, inside, outside, and HA interfaces.

  Note The management and HA interfaces must use different port profiles.

Step 7 In the Summary screen, confirm that the information is accurate, and then click **Finish**.

Step 8 If you instantiated the ASA 1000V from a service image, you must do the following to ensure registration with Prime Network Services Controller:

a) **Within 15 minutes of instantiation**, manually register the ASA 1000V to Prime Network Services Controller by using the ASA 1000V CLI.

b) If you do not register the ASA 1000V within 15 minutes of instantiation, the instantiated ASA 1000V will enter a failed state, and you must delete it manually from Prime Network Services Controller and the hypervisor.

Field Descriptions

Properties Screen

Field	Description
Name	Edge firewall name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, period, and colon. You cannot change this name after it is created.
Description	Edge firewall description.
Host Name	Management hostname of the firewall.
High Availability	Check the **Enable HA** check box to enable high availability.
Device Configuration Profile	Do either of the following: • Click the profile name to view and optionally modify the currently assigned device configuration profile. • Click **Select** to choose a different device configuration profile.
Device Service Profile	Do either of the following: • Click the profile name to view and optionally modify the currently assigned device service profile. • Click **Select** to choose a different device service profile.

Unassigning an ASA 1000V

If required, you can unassign an ASA 1000V from an edge firewall.

SUMMARY STEPS

1. Choose **Resource Management > Managed Resources > root >** *tenant*.
2. In the Network Services tab, choose the required edge firewall.
3. In the toolbar, choose **Actions > Unassign ASA 1000V**.
4. When prompted, confirm the action.

DETAILED STEPS

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant*.

Step 2 In the Network Services tab, choose the required edge firewall.

Step 3 In the toolbar, choose **Actions > Unassign ASA 1000V**.

Step 4 When prompted, confirm the action.

Edge Routers

Edge Router Configuration Workflow

This workflow describes how to create an edge router under a tenant.

Steps	Notes
1. Confirm that prerequisites are met.	See Prerequisites for Configuring Edge Routers, on page 212.
2. (Optional) Configure Edge Router configuration and service profiles and policies. If needed, you can use the default profiles.	• Choose **Policy Management > Service Profiles > *tenant* > Edge Router** and select **Device Service Profiles** or **Interface Service Profiles** • Choose **Policy Management > Service Policies > *tenant*** and select **Policies** or **Policy Helpers**
3. Add an edge router under a tenant.	Choose **Resource Management > Managed Resources > *tenant*** and select **Add Edge Router** from the Network Services Actions drop-down list.
4. Enter the appropriate information in the Add Edge Router Wizard.	See Adding Edge Routers, on page 213.
5. Verify that the edge router has been created.	Choose **Resource Management > Resources** and select the edge router device and view the device status in the table. It takes some time for the logical device to associate with the physical device.

Prerequisites for Configuring Edge Routers

The following table lists the information you should have on hand and any prerequisites for configuring edge routers. For information on adding and configuring edge routers, see Edge Router Configuration Workflow, on page 211 and Adding Edge Routers, on page 213.

Note By default, CSR 1000V OVA images contain three vNICs and will instantiate CSR 1000V service images with only three interfaces. If you need more than three edge router interfaces, see http://www.cisco.com/en/US/docs/routers/csr1000/software/configuration/vminterface.html for information on how to configure additional interfaces.

Item	Notes
Decide whether you are assigning or instantiating an edge router.	Note all the necessary edge router information needed for configuration. • To assign an edge router to , an edge router VM must be installed. Use VM management software (such as VMware) to deploy a device image from an OVA template and register the device with . For Cisco Cloud Services Router 1000V, see the Cisco CSR 1000V Configuration Guide. • To instantiate an edge router, an edge router service image must be available. For more information, see Importing Service Images, on page 200.
At least one tenant is configured	See Creating a Tenant.
Determine the number of loopback interfaces required on the edge router.	Loopback interfaces cannot be added or deleted after an edge router is instantiated. Therefore, all required loopback interfaces must be configured before assignment or during instantiation.
Determine the number of data (Gigabit Ethernet) interfaces required on the edge router.	Data interfaces cannot be added or deleted after an edge router is instantiated. Therefore, all required data interfaces must be configured before assignment or during instantiation.
Decide whether to create a new edge router device profile	offers a default configuration profile that contains common policies for all devices managed in . You can use or edit the default profile, or customize a new profile. To create a new device configuration profile, choose **Policy Management > Device Configurations > *root* (or *tenant*) > Device Profiles** and click **Add Device Profile**.

Item	Notes
Decide whether to configure or use the default device service profiles.	To create or edit a device service profile, note the following applicable router policy and interface information you need for configuration: **Device Service Profile (Policies)** • Routing Policy: Static, BGP, or OSPF • NAT **Note** Edge routers support a limited set of NAT policy options. • Zone-Based Firewall **Note** For more information on zone-based firewall configuration, see Configuring Zone-Based Firewall Policies, on page 119. **Note** A zone policy defines the traffic that you want to allow or deny between zones. A zone-pair policy allows you to specify a unidirectional firewall policy between two zones. The direction is defined by specifying a source and destination zone. **Interface Service Profiles** • Ingress • Egress • NAT Membership • Firewall Zone Membership **Note** A firewall zone is a group of interfaces to which a policy can be applied. By default, traffic can flow freely within that zone but all traffic to and from that zone is dropped. To allow traffic to pass between zones, you must explicitly declare it by creating a zone-pair and a policy for that zone.

Adding Edge Routers

This procedure describes the steps in the Add Edge Router wizard. The Add Edge Router wizard is part of the Edge Router Configuration Workflow, on page 211. Before using the Add Edge Router wizard, see Prerequisites for Configuring Edge Routers, on page 212.

SUMMARY STEPS

1. Choose **Resource Management > Managed Resources >** *tenant*, and then choose **Add Edge Router**.
2. Enter edge router device information in the Properties window and click **Next**.
3. If you are instantiating an edge router, do the following, and then click **Next**:
4. In the Service Device screen, if you are assigning an edge router, choose the deployed edge router, configure the applicable interfaces and IP addresses, and then click **OK**.
5. In the Placement screen, choose the location for the edge router.
6. In the Interface screen, assign the IP address. Keep in mind that the primary IP address and the submanagement IP address must be in the same subnet.
7. Click **Finish** if the summary details are correct.

DETAILED STEPS

Step 1 Choose **Resource Management > Managed Resources >** *tenant*, and then choose **Add Edge Router**.

Step 2 Enter edge router device information in the Properties window and click **Next**.

Step 3 If you are instantiating an edge router, do the following, and then click **Next**:

a) Select the image to use to instantiate the edge router.
b) In the Compute area, enter the number of virtual CPUs and amount of memory you need to meet the required throughput.
c) In the VM Access area, enter the access credentials.

Step 4 In the Service Device screen, if you are assigning an edge router, choose the deployed edge router, configure the applicable interfaces and IP addresses, and then click **OK**.

Note
- You must configure at least two Gigabit interfaces.
- The primary IP address and the sub management IP address must be in the same subnet.

Step 5 In the Placement screen, choose the location for the edge router.

Step 6 In the Interface screen, assign the IP address. Keep in mind that the primary IP address and the submanagement IP address must be in the same subnet.

Step 7 Click **Finish** if the summary details are correct.

Edge Router Deployment Options

Edge routers can support different amounts of throughput based on the number of virtual CPUs and amount of memory. Choose the number of virtual CPUs and amount of memory that are appropriate for your environment and the desired throughput.

Throughput	Technology Package		
Speed	Standard	Advanced	Premium
10 Mbps	1 vCPU, 2.5 GB RAM	1 vCPU, 2.5 GB RAM	1 vCPU, 2.5 GB RAM

Throughput	Technology Package		
50 Mbps	1 vCPU, 2.5 GB RAM	1 vCPU, 2.5 GB RAM	1 vCPU, 2.5 GB RAM
100 Mbps	1 vCPU, 2.5 GB RAM	1 vCPU, 2.5 GB RAM	1 vCPU, 2.5 GB RAM
250 Mbps	4 vCPU, 4 GB RAM	4 vCPU, 4 GB RAM	4 vCPU, 4 GB RAM
500 Mbps	4 vCPU, 4 GB RAM	—	—
1 Gbps	4 vCPU, 4 GB RAM	—	—

Managing Edge Routers

You can do the following edge router management tasks:

- Edit information and network interfaces.
- Modify the device profile, device service profile, and the interface service profile.
- Delete an edge router.
- Monitor status and view fault information.
- Start, stop, and reboot edge routers that have been instantiated.
- Perform assign and unassign operations for edge routers that have been registered.

For information on initial edge router configuration, see Edge Router Configuration Workflow, on page 211 and Prerequisites for Configuring Edge Routers, on page 212.

SUMMARY STEPS

1. Choose **Resource Management > Managed Resources > root >** *tenant*.
2. In the Network Services tab, right-click the required edge router and select the operation you want to perform.
3. If you chose **Edit**, modify or view the appropriate tab information in the Edit dialog box, and then click **OK**.

DETAILED STEPS

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant*.

Step 2 In the Network Services tab, right-click the required edge router and select the operation you want to perform.

Step 3 If you chose **Edit**, modify or view the appropriate tab information in the Edit dialog box, and then click **OK**.

Note To view additional information about an entry in the Faults tab, double-click the entry, or select the entry and then click **Properties**.

Load Balancers

Load Balancer Configuration Workflow

This workflow describes how to create a load balancer under a tenant. The workflow includes creating a virtual server profile and an associated service if one does not exist.

Steps	Notes
1. Confirm that the prerequisites are met.	See Prerequisites for Configuring Load Balancers, on page 216. This topic also includes the following information: • Importing load balancer licenses. • Installing the device adapter.
2. Add a virtual server profile to a tenant.	Add a service and enter general and server farm information. See Load Balancing Service Dialog Boxes, on page 219 for server farm information.
3. Verify that the virtual server profile has been created.	Choose **Policy Management > Service Profiles >** ***tenant*** **> Load Balancer** and confirm that the virtual server has been created in the Virtual Server Profiles table.
4. Add a load balancer device under a tenant.	Choose **Resource Management > Managed Resources >** ***tenant*** and then choose **Add Load Balancer** from the Network Services Actions drop-down list.
5. Enter the appropriate information in the Add Load Balancer Wizard.	The wizard maps a logical load balancer and configures the virtual IP addresses to the selected virtual servers. For more information, see Adding Load Balancers, on page 218.
6. Verify that the load balancer has been created.	Choose **Resource Management > Resources > VPX >** *load-balancer* and then view the device status in the table. It takes some time for the logical device to associate with the physical device.

After a load balancer is added and configured, you can view faults, edit, and monitor the load balancer. For more information, see Managing Load Balancers, on page 221. Also, if you would like to edit services on a server profile (for example, add ping monitors), choose **Policy Management > Service Profiles >** ***tenant*** **> Load Balancer > Virtual Server Profiles >** ***service*** and click **Edit**.

Prerequisites for Configuring Load Balancers

The following table lists the information you should have on hand and any prerequisites for configuring load balancers.

Note For load balancer configuration, see Load Balancer Configuration Workflow, on page 216 and Adding Load Balancers, on page 218.

Item	Notes
Tenant	At least one existing tenant configured.
Load Balancer Information	
For Citrix NetScaler load balancers, the Prime Network Services Controller Device Adapter must be deployed	See "Installing the Prime Network Services Controller Device Adapter for Load Balancers."
Decide whether you are assigning or instantiating a load balancer	Note all the necessary load balancer information needed before configuration. To assign a load balancer, the load balancer OVA must first be deployed. For Citrix NetScaler load balancers, see the Citrix Netscaler documentation. To instantiate a load balancer, a load balancer service image must be available. See Importing Service Images, on page 200.
Virtual Server Profile Information	
Determine the number of virtual servers required on the load balancer	Virtual servers cannot be added or deleted after a load balancer is instantiated. All required virtual servers must be configured before registration or during instantiation.
Service and server farm information	• Protocol • Port • Algorithm • Persistence • Real server • Hostname or IP address For more information, see Load Balancing Service Dialog Boxes, on page 219.
Monitor information	• TCP • HTTP • Ping

Adding Load Balancers

This procedure describes the steps in the Add Load Balancer wizard. Before using the Add Load Balancer wizard, confirm that the prerequisites are met in Prerequisites for Configuring Load Balancers, and see Load Balancer Configuration Workflow.

SUMMARY STEPS

1. Enter load balancer device information in the Properties window and click **Next**.
2. Choose whether you want to register or instantiate a load balancer in the Service Device window.
3. Do one of the following:
4. Configure a virtual server by selecting an existing virtual server profile and assigning virtual IP addresses (VIPs) in the Configure Virtual Server window, then click **Next**.
5. Click **Finish** if the summary details are correct.

DETAILED STEPS

Step 1 Enter load balancer device information in the Properties window and click **Next**.

Note If you choose to enable vPath, only vPath-enabled devices (like Citrix Netscaler 1000V) will be available for selection in the instantiation image list.

Step 2 Choose whether you want to register or instantiate a load balancer in the Service Device window.

Step 3 Do one of the following:

1 If you are registering a load balancer:

- Enter all required information (device IP address, subnet mask and gateway information).
- Select the device type and version from the drop-down lists.
- Enter the device access credentials.
- Configure one data interface and one virtual IP interface in the Configure Interface window, then click **Next**. All interfaces must be in different subnetworks. The management interface is automatically taken from the device IP address that you entered above.

2 If you are instantiating a load balancer:

- Select the instantiation image and locate where the VM will be hosted.
- Enter the virtual machine access credentials and click **Next**.
- Navigate to VM placement.
- Configure one data interface and one management interface in the Configure Interface window, then click **Next**.

Step 4 Configure a virtual server by selecting an existing virtual server profile and assigning virtual IP addresses (VIPs) in the Configure Virtual Server window, then click **Next**.

Note
- VIPS are public IP addresses that clients connect to and where all traffic is directed to. Behind VIPs are real servers where load balancing occurs. Limit the number of VIPs to 64 VIPs per load balancer.
- The VIP IP address cannot be on the management network.

Step 5 Click **Finish** if the summary details are correct.

For troubleshooting information, view errors in the Faults tab (see Managing Load Balancers). If you would like to modify the virtual server profile services (for example, add monitors to your server farm) choose **Policy Management > Service Profiles >** ***tenant*** **> Load Balancer > Virtual Server Profiles >** ***service*** and click **Edit**. Navigate to the Server Farm tab to modify any information.

Load Balancing Service Dialog Boxes

Various Service dialog boxes appear when configuring a virtual server service for a load balancer profile. For more information on how to configure a load balancer profile, see the Load Balancer Configuration Workflow topic.

Server Farm Information

Note

- If you need to add a new server farm, you must enter information in the Real Server and Monitor tabs.
- To confirm that your configurations were applied, you can view the device's UI.

Field	Notes
Protocol	If you select SSL or SSL_TCP, a security policy must be configured. See the Security Policy Dialog Boxes topic which describes.
Algorithm	Select the scheduling algorithm for the server farm. • Least Connection—New connections are sent to the server with the fewest connections. • Destination IP Hash—Selects a server based on a hash of the source IP address of each packet. • Least Bandwidth—New connections are sent to the server with the least bandwidth. • Least Packets—New connections are sent to the server with the least packets. • Least Response Time—New connections are sent to the server with the least response time. • Round Robin—Each server is used in turn according to the weight assigned to it. • URL Hash—The left part of the URL (before the question mark) is hashed and divided by the total weight of the running servers. The result designates which server will receive the request. Applicable to only HTTP service load balancing.

Field	Notes
Increment Interval	Interval at which the server is pinged.
Persistence	Select the persistence method that will define how the load balance service handles information. The following persistence restrictions exist: • SSL—Applies only to SSL-based services. • Cookie Insert—Applies only to HTTP-based services. If the service protocol and persistence is an invalid combination, a "failed-to-apply" status appears in the Network Services tab.
Monitors	
HTTP	Monitors HTTP traffic.
Ping	Pings real servers to see if they are up and running.
TCP	Monitors TCP traffic.

Limitations

- 64 real servers per server farm
- 64 monitors per server farm
- 16 services per virtual server

Security Policy Dialog Boxes

Load Balancing Security Policy Information

For load balancing, if SSL and SSL-TCP protocols are selected, security policies must be configured. You can configure security policies so that cryptographic authentication is enabled using the SSL Params, Cipher Groups, Certificate, and Certificate Key File dialog boxes.

Note SSL offload configuration requires a valid certificate and key file.

Dialog Box	Description
SSL Params	Allows you to customize the SSL configuration. From this dialog box you may choose to enable and configure the following: • Ephemeral RSA • Session reuse • Cipher redirect • SSL and SSLv2 redirect • Selection of TLSv1, SSLv3, and SSLv2 protocols • Close notifications • SSL redirect port rewrite
Cipher Group	Allows you to select or add cipher groups. A cipher group is a set of cipher suites that you attach to an SSL service.
Certificate and Certificate Key File	Allows you to configure or add certificates and certificate key files.

Managing Load Balancers

You can do the following load balancer management tasks:

- Edit information and network interfaces. (Management and data IP interfaces cannot be modified after creation.)
- Delete a load balancer.
- Monitor status and view fault information.

SUMMARY STEPS

1. Choose **Resource Management > Managed Resources > root >** *tenant*.
2. In the Network Services tab, choose the required load balancer, and then click **Edit** or **Delete**.
3. If you chose **Edit**, modify or view the appropriate tab information in the Edit dialog box, and then click **OK**.

DETAILED STEPS

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant*.

Step 2 In the Network Services tab, choose the required load balancer, and then click **Edit** or **Delete**.

Step 3 If you chose **Edit**, modify or view the appropriate tab information in the Edit dialog box, and then click **OK**.

Note To view additional information about an entry in the Faults tab, double-click the entry, or select the entry and then click **Properties**.

If you would like to modify the virtual server profile services (for example, add monitors to your server farm) choose **Policy Management > Service Profiles >** ***tenant*** **> Load Balancer > Virtual Server Profiles >** ***service*** and click **Edit**. Navigate to the Server Farm tab to modify any information.

Adding a Port Profile to a VSM

enables you to add a port profile to an enterprise VSM. You cannot add a port profile to a cloud VSM.

If an enterprise VSM has preconfigured port profiles or virtual service configurations that were created outside of , these configurations will not be displayed in the GUI.

If you create a port profile in and specify a VLAN, you must create the VLAN itself on the VSM and then add it to the necessary system and uplink port profiles. The same steps apply for VLANs that you specify while creating service devices, such as edge or compute firewalls: you must create the VLANs on the devices, and then add them to the appropriate system and uplink port profiles.

Before You Begin

Confirm the following:

- An enterprise VSM is registered and in the *applied* state in by choosing **Resource Management > Resources > VSMs**.
- You have admin privileges.

SUMMARY STEPS

1. Choose **Resource Management > Resources > VSMs >** *vsm*, then click **Edit**.
2. Above the Port Profile table, click **Add**.
3. In the Add Port Profile dialog box, enter the required information as follows, then click **OK**:

DETAILED STEPS

Step 1 Choose **Resource Management > Resources > VSMs >** *vsm*, then click **Edit**.

Step 2 Above the Port Profile table, click **Add**.

Step 3 In the Add Port Profile dialog box, enter the required information as follows, then click **OK**:

1 In the General tab, provide the following information:

- Name
- Description
- State: Enabled or Disabled.
- Type of Binding: Dynamic, Ephemeral, or Static.
- Binding Option: Auto, AutoExpand, or None.

- Maximum and minimum number of ports.
- Tenant or subordinate organization in which to create the port profile.

2 In the L2 Network Membership tab, provide the following information:

- Capability: Bridge Domain or VLAN.
- Mode: Access or Trunk
- VLAN number (Access mode) or VLAN range (Trunk mode).

The NICs table is populated automatically after you bind a service path to the port profile and the service path is used the first time. For more information about configuring a service path and binding it to a port profile, see Service Path Configuration Workflow, on page 75.

Updating Discovered VSM Port Profiles

When discovers a VSM port profile that was configured directly on the Nexus 1000V, only some of the configuration information is available to . As a result, you need to provide the missing information in .

This situation usually occurs under the following circumstances:

- A VSM port profile with an organization and virtual service have been configured on a Nexus 1000V.
- VMs with vNICs that use the port profile have also been configured on the device.

SUMMARY STEPS

1. Log in to the GUI and choose **Resource Management > Resources > VSM**.
2. Choose the VSM with the port profile that was configured using the CLI, and then click **Edit**.
3. In the Port Profiles table, choose the required port profile, and then click **Edit**.
4. Update the port profile properties so that they are consistent with the configured port profile, and save your changes. You can then use the port profile as needed.
5. If any port profile properties are modified via the CLI, update them in so that the configurations remain synchronized.

DETAILED STEPS

Step 1 Log in to the GUI and choose **Resource Management > Resources > VSM**.

Step 2 Choose the VSM with the port profile that was configured using the CLI, and then click **Edit**.

Step 3 In the Port Profiles table, choose the required port profile, and then click **Edit**.

Step 4 Update the port profile properties so that they are consistent with the configured port profile, and save your changes. You can then use the port profile as needed.

Step 5 If any port profile properties are modified via the CLI, update them in so that the configurations remain synchronized.

Troubleshooting Devices and Services

You can use to troubleshoot faults associated with managed devices and services.

SUMMARY STEPS

1. Choose **Resource Management > Managed Resources > root >** *tenant*.
2. In the Network Services tab, choose the required service or device, and then click **Edit**.
3. In the General tab, review the Status area for any issues or states affecting reachability, configuration, or association.
4. In the Faults tab, review the displayed faults. To view additional information about a fault, double-click the entry, or choose the entry and then click **Properties**.

DETAILED STEPS

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant*.

Step 2 In the Network Services tab, choose the required service or device, and then click **Edit**.

Step 3 In the General tab, review the Status area for any issues or states affecting reachability, configuration, or association.

Step 4 In the Faults tab, review the displayed faults. To view additional information about a fault, double-click the entry, or choose the entry and then click **Properties**.

Launching ASDM

enables you to launch Cisco Adaptive Security Device Manager (ASDM) as a Web Start application on your desktop.

You can set up ASDM to be used by the ASA 1000V when it is configured for either management mode or ASDM management mode. When the ASA 1000V is configured to use management mode, you can use ASDM to monitor the status of the ASA 1000V, but you cannot use it to manage configurations.

Before You Begin

You must complete the following tasks before launching ASDM from :

1 Do one of the following:

- If you have not already deployed the ASA 1000V OVA, do so; during the deployment, provide the ASDM client IP address.
- If you have already deployed the ASA 1000V OVA, apply the following configuration by using the VM console in the vSphere client:
  - Add a route on the management interface to the ASDM client subnet by issuing the following command:
    ```
    ASA1000V(config)# route interface ip subnet next-hop-ip
    ```
    where *interface* is the management interface to the ASDM client subnet, *ip* is the IP address of the host that accesses ASDM, *subnet* is the ASDM client subnet, and *next-hop-ip* is the IP address of the gateway.

    Note Perform this step only if the next hop gateway IP address was not specified when deploying the ASA 1000V.

  - Allow HTTP access via the management interface for the ASDM client subnet by entering the following command:
    ```
    ASA1000V(config)# http ip subnet interface
    ```
    where *ip* is the IP address of the host that accesses ASDM, and *interface* is the ASDM client interface.

    Note Perform this step only if the ASDM client IP address was not specified when deploying the ASA 1000V.

2 Confirm the following:

- The ASA 1000V is registered to .
- A valid username and password exist for the ASA 1000V VM console.

3 Assign the edge firewall to an ASA 1000V instance. If the edge firewall is not assigned to an ASA 1000V instance, the ASDM options are not displayed in the UI.

4 Confirm that your system is configured to run downloaded Java Web Start applications.

For more information about configuring ASDM, see the *Cisco ASA 1000V Cloud Firewall Getting Started Guide*.

SUMMARY STEPS

1. Choose **Resource Management > Managed Resources >** *tenant*.
2. In the Network Services tab, choose the required edge firewall, and then click **Edit**.
3. In the Edit dialog box, click **Launch ASDM**.
4. In the ASDM Launch screen, click **Run ASDM**.

DETAILED STEPS

Step 1 Choose **Resource Management > Managed Resources >** *tenant*.

Step 2 In the Network Services tab, choose the required edge firewall, and then click **Edit**.

Step 3 In the Edit dialog box, click **Launch ASDM**.
The ASDM Launch screen opens.

Step 4 In the ASDM Launch screen, click **Run ASDM**.
The ASDM Web Start application is automatically downloaded and runs. If prompted, accept the certificates.
Note If an ASDM login dialog box is displayed, you can click **OK** without entering login credentials.

Managing VSG Pools

Adding a VSG Pool

SUMMARY STEPS

1. Choose **Resource Management > Managed Resources > root >** *tenant*.
2. In the VSG Pools tab, click **Add Pool**.
3. In the Add Pool dialog box, enter a name and description for the pool.
4. To assign members to the pool:
5. Click **OK**.

DETAILED STEPS

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant*.

Step 2 In the VSG Pools tab, click **Add Pool**.

Step 3 In the Add Pool dialog box, enter a name and description for the pool.

Step 4 To assign members to the pool:

a) Click **(Un)Assign**.
b) In the Available list, choose the VSGs that you want to add to the pool, and then click the arrow to move them to the Assigned list.
c) Click **OK**.

Step 5 Click **OK**.

Assigning a VSG Pool

You can assign a VSG pool to a compute firewall when you add a compute firewall to a tenant or other organization. For information on assigning a VSG to a compute firewall, see Adding a Compute Firewall, on page 201.

Editing a VSG Pool

After you create a VSG pool, you can change its description and add or remove VSGs from the pool as required.

SUMMARY STEPS

1. Choose **Resource Management > Managed Resources > root >** *tenant*.
2. In the VSG Pools tab, choose the pool that you want to edit, and then click **Edit**.
3. In the Edit Pool dialog box, modify the following information as required, and then click **OK**:

DETAILED STEPS

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant*.

Step 2 In the VSG Pools tab, choose the pool that you want to edit, and then click **Edit**.

Step 3 In the Edit Pool dialog box, modify the following information as required, and then click **OK**:

a) Edit the description.
b) To add or remove VSGs from the pool, click **(Un)Assign**.
c) To delete a VSG from the pool, choose the required VSG from the list of pool members, and then click **Delete**.

Unassigning a VSG Pool

If required, you can unassign a pool from a compute firewall.

SUMMARY STEPS

1. Choose **Resource Management > Managed Resources > root >** *tenant*.
2. In the Network Services tab, select the required firewall, and then choose **Actions > Unassign VSG/Pool**.
3. When prompted, confirm the action.

DETAILED STEPS

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant*.
Step 2 In the Network Services tab, select the required firewall, and then choose **Actions > Unassign VSG/Pool**.
Step 3 When prompted, confirm the action.

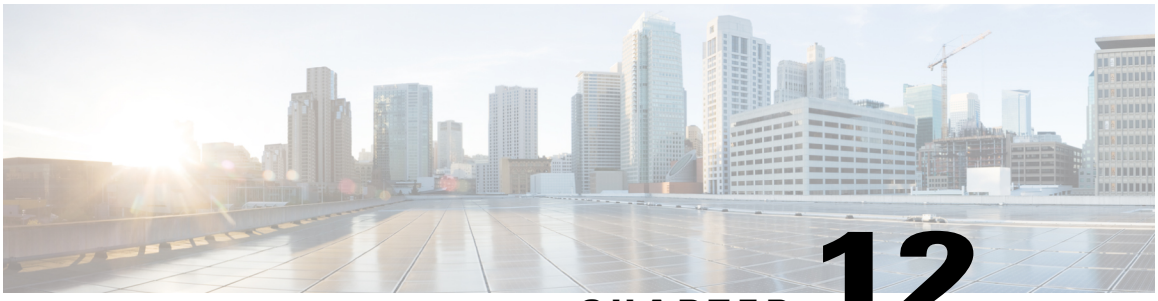
Deleting a VSG Pool

SUMMARY STEPS

1. Choose **Resource Management > Managed Resources > root >** *tenant*.
2. In the VSG Pools tab, choose the pool that you want to delete, and then click **Delete**.
3. When prompted, confirm the deletion.

DETAILED STEPS

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant*.
Step 2 In the VSG Pools tab, choose the pool that you want to delete, and then click **Delete**.
Step 3 When prompted, confirm the deletion.



CHAPTER 12

Integrating with DCNM

This section includes the following topics:

- DCNM Integration Overview, page 229
- Configuring Connectivity with DCNM, page 232
- Troubleshooting Integration Issues, page 233

DCNM Integration Overview

supports integration with Cisco Data Center Network Manager (DCNM). As part of this integration, provides the automation of virtual network services in Cisco Dynamic Fabric Automation (DFA). In the Cisco DFA solution, services like firewalls and load balancers are deployed at leaf nodes within the spine-leaf topology and in border leaf nodes, in contrast to more traditional data centers where these services are deployed at the aggregation layer.

The following table describes the primary items in the integration with DCNM:

Item	Description
	Provides central management of network services in a multi-tenant environment.
DCNM	• Provides the setup, visualization, management, and monitoring of the data center infrastructure. • Provides configuration and image management for the fabric.
Dynamic Fabric Automation (DFA) cluster	Provides a simplified spine-leaf architecture, enhanced forwarding, and distributed control plane.

Item	Description
Adaptor	• Links with DCNM. • Enables DCNM to interoperate with one or more instances of . • Maps the tenants and virtual data centers to the instances responsible for network services. • Listens to network database updates and communicates those updates to the appropriate instance. • Upon notification of a new network service in a tenant network, notifies DCNM of the change.

provides centralized management of network services by supporting the following actions:

- The creation, reading, updating, and deletion of vPath-based service chains.
- The creation, updating, and deletion of network services.
- Communicating changes about network services to the Adapter.

The GUI reflects this support by displaying information for networks and subnetworks associated with a tenant, and network services in a tenant's network.

Terminology

The following table identifies the corresponding terms in and DCNM:

Prime Network Services Controller Name	DCNM Name	Description
Tenant	Organization	A collection of VDCs for tenant-level separation of resources and data.
Virtual Data Center (VDC)	Partition	An independent routing domain that includes a collection of subnetworks. A VDC can belong to only one tenant.
Subnetwork	Network	A Layer 2 network with a unique identifier. A subnetwork can belong to only one VDC.

Networks

After an admin user provisions one or more tenant networks in DCNM, DCNM sends the information about the tenant network to . A tenant-admin user in can then deploy network services such as firewalls, load balancers, and routers on those networks.

For each network, DCNM provides with a *handle* that uniquely identifies the network on a VM manager and the network's Layer 3 IP details, such as subnet prefix, mask, and default gateway.

To view these networks in , choose **Resource Management > Managed Resources > root >** *tenant (or other subordinate organization)*, and then click the **Subnetworks** tab.

You can place the interfaces of a network service that is deployed at a particular level (or *node*) in the tenant organizational hierarchy on available networks at the following locations:

- The organization node on which the service is being deployed.
- Organization nodes that are children of the organization node on which the service is being deployed.
- Organization nodes that are ancestors of the organization node on which the service is being deployed.

Network Roles

Networks are qualified by a role property which identifies their intended usage. The following table describes the various network roles.

Network Role	Description
Host	Tenant-specific network intended for tenant application VMs. Service nodes can also be connected to this network.
Service	Tenant network intended exclusively for service nodes.
External	Tenant network that provides external connectivity. Both tenant application VMs and service nodes can connect to this network.
Management	Shared infrastructure network used for communication between service nodes and . Service node management interfaces connect to this network.
HA	Shared infrastructure network intended for high availability communications between service nodes. Service node HA interfaces connect to this network.

In contrast with tenant networks, which are tenant-specific and provisioned on the data center fabric by DCNM, infrastructure networks are shared by all tenants and are provisioned on the data center fabric out of band.

Details about infrastructure networks need to be added to by the admin user. Because these networks are shared, they can be added only to root (**Tenant Management > root**).

To add details about infrastructure networks, choose **Resource Management > Managed Resources** and then click the **Subnetworks** tab.

Roles and Privileges

The following roles support integration with DCNM:

Role	Responsibility
admin	• Deploy if it is not already deployed. • Configure the instance and credentials on DCNM. • Confirm communication between and DCNM. • As needed, create tenant-admin user accounts. • Provide the tenant-admin user with the management IP address.

Role	Responsibility
tenant-admin	• Add, modify, or delete network services in the scope of the tenant organizational hierarchy provided by DCNM. • As part of network service creation, connect the data interfaces on the subnetworks for that tenant.

Configuring Connectivity with DCNM

This procedure describes how to configure connectivity between and DCNM.

After you have successfully configured connectivity, the following aspects apply:

- When operating with DCNM, you cannot create, modify, or delete tenants or virtual data centers from the GUI.
- allows admin and tenant-admin users to create, modify, and delete Application and Tier organizational levels under a Virtual Data Center organization.
- The GUI does not allow admin or tenant-admin users to modify any information related to tenant-scoped network or subnetworks. This restriction does not apply to management or HA networks and subnetworks that are managed by admin users.
- If you create, update, or delete a network service in , it will be reflected in both DCNM and .

Before You Begin

Confirm the following:

- The DCNM system is running.
- Enhanced Fabric Network was enabled during DCNM deployment.
- You have network access to the DCNM system.
- You have the appropriate privileges for configuring DCNM.
- You have deployed in Orchestrator mode.
- You have created a user account with the admin role for use only by the Adaptor in DCNM.

For more information about these prerequisites, see the following links:

- Cisco Prime Data Center Network Manager—http://www.cisco.com/en/US/products/ps9369/tsd_products_support_series_home.html
- Prime Network Services Controller Quick Start Guide—http://www.cisco.com/en/US/products/ps13213/prod_installation_guides_list.html

SUMMARY STEPS

1. Log in to the DCNM VM console as root.
2. Navigate to the /opt/nscadapter/bin directory.
3. Start the adaptor by entering the following command: **nsc-adapter-mgr adapter start**
4. Using the **nsc-adapter-mgr nsc add** command, enter the following information to provide DCNM with access to :
5. Log in to the Cisco DCNM GUI and do the following:
6. To confirm that connectivity is established between DCNM and , log in to and confirm that the organization is displayed in the Tenant Management tab.

DETAILED STEPS

Step 1 Log in to the DCNM VM console as root.

Step 2 Navigate to the /opt/nscadapter/bin directory.

Step 3 Start the adaptor by entering the following command: **nsc-adapter-mgr adapter start**

Step 4 Using the **nsc-adapter-mgr nsc add** command, enter the following information to provide DCNM with access to :

- management IP address
- Username for access
- Password for access

The command format is **nsc-adapter-mgr nsc add** *ip-address username password*.

Step 5 Log in to the Cisco DCNM GUI and do the following:

a) Choose **Admin > Dynamic Fabric Automation > Settings**.
b) Choose **Config > Dynamic Fabric Automation (DFA) > Auto-Configuration**.
c) Click **Add Organization** and enter the information for the organization. An organization in DCNM corresponds to a tenant in .
d) As needed, add partitions to the organization. A partition in DCNM corresponds to virtual data center in .
e) Add a network to the partition.

Step 6 To confirm that connectivity is established between DCNM and , log in to and confirm that the organization is displayed in the Tenant Management tab.

Troubleshooting Integration Issues

If you encounter issues with the and DCNM integration, you can look for information in the following locations:

- On the DCNM server, review the log files in /opt/nscadapter/var/log for information.
- In the GUI:

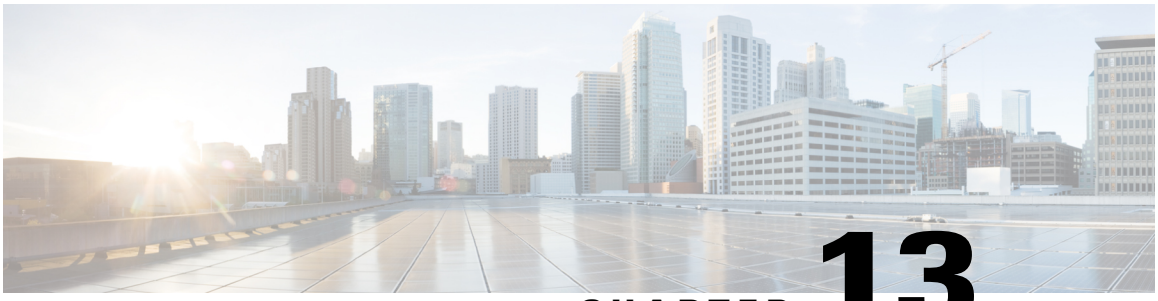
- Review faults for services by choosing **Resource Management > Managed Resources > root >** *tenant* **> Network Services >** *network-service* **> Edit > Faults** tab.
- Review audit logs and faults by choosing **Resource Management > Diagnostics > Audit Logs** or **Faults**.

For either option, double-click a fault to view more information.

The following table describes specific issues that you might encounter and how to address them:

Symptom	Cause	Resolution
Organizations and partitions are created in DCNM but no tenants or virtual device contexts (VDCs) are displayed in	The configurations in DCNM and are incomplete.	1 Confirm that the Service Configuration parameters are complete for networks created in DCNM. 2 Confirm that is registered with the VM Manager IP parameter.
Networks are created in DCNM but no tenants, VDCs, or subnetworks are displayed in .	The Network Services Controller (NSC) Adapter does not have an active connection to .	Use the **nsc-adapter-mgr adapter connections** command to ensure there is an active connection to .
	The NSC Adapter is not active on DCNM.	Use the **nsc-adapter-mgr adapter connections** command to ensure there is an active connection to DCNM.
	does not have the VM Manager IP.	Confirm that is registered with the correct VM Manager and provide the VM Manager IP address in the VM Manager IP parameter.
	Networks were added to DCNM while or the NSC Adapter was down.	1 Enter the command **nsc-adapter-mgr adapter connections** and verify that the connections are correct. 2 In the DCNM GUI, choose the auto-config interface, choose the network, click **Edit**, and then click **OK** without making changes.

Symptom	Cause	Resolution
Service networks were deleted in DCNM but the tenants, VDCs, and subnetworks are still shown in .	Networks were deleted from DCNM while or the NSC Adapter was down.	1 Enter the **nsc-adapter-mgr adapter connections** command and verify that the connections are correct. 2 In the DCNM GUI, choose the auto-config interface, choose the network, click **Edit**, and then click **OK** without making changes.
An edge service was removed from but the Service Node IP Address is still shown in DCNM.	The service was deleted from while DCNM or the NSC Adapter was down.	Manually delete the Service Node IP Address in DCNM for the affected partition.
An edge service was deployed in but the Service Node IP Address is not shown in DCNM.	The service was deployed in while DCNM or the NSC Adapter was down.	Manually update the Service Node IP Address in DCNM auto-config for the affected partition.
Host traffic does not reach the service node.	• The wrong profile is specified in DCNM for host networks. • The service is not attached to the leaf.	• Make sure that the correct profile is specified in DCNM for the host network. • Make sure that the auto-config profile and parameters are correct with particular attention to the Service Node IP address.



CHAPTER 13

Configuring Administrative Operations

This section includes the following topics:

- Administrative Operation Conventions, page 237
- Managing Backup Operations, page 237
- Restoring a Backup Configuration, page 242
- Managing Export Operations, page 246
- Configuring Import Operations, page 250

Administrative Operation Conventions

The following conventions apply when performing the administrative operations described in this section:

- The remote file location you specify must start with a slash (/) and include the full path and file name. Do not use relative paths.
- The user name and password on the remote system must be correct, and the user specified must have read and write permissions on the remote system.
- The file on the remote system must be a valid file, and the size cannot be zero.
- For backup and export operations, if the Task tab contains a Remote Err Description of *No such file*, reboot the VM via vCenter.

Managing Backup Operations

We recommend that you use backup and restore operation as a disaster recovery mechanism. To migrate configuration data from one server to another, use export and import operations.

Creating a Backup Operation

Before You Begin

Obtain the backup server IP address or hostname and authentication credentials.

SUMMARY STEPS

1. Choose **Administration** > **Operations**.
2. Click **Create Backup Operation**.
3. In the Create Backup Operation dialog box, complete the following fields, then click **OK**:

DETAILED STEPS

Step 1 Choose **Administration** > **Operations**.

Step 2 Click **Create Backup Operation**.

Step 3 In the Create Backup Operation dialog box, complete the following fields, then click **OK**:

Field	Description
Admin State	One of the following administrative states: • enabled—Backup is enabled. The system runs the backup operation when you click **OK**. • disabled—Backup is disabled. The system does not run the backup operation when you click **OK**. If you choose this option, all fields in the dialog box remain visible.
Type	Backup type. The backup 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 system. This field is not editable.
Protocol	Protocol used when communicating with the remote server: • FTP • SCP • SFTP
Hostname/IP Address	Hostname or IP address of the device where the backup file is stored. This entry cannot be changed when editing the operation. If you use a hostname instead of an IP address, you must configure a DNS server.
User	Username the system uses to log into the remote server.

Field	Description
Password	Password the system uses to log into the remote server. This field is displayed if you choose **enabled** in the Admin State field. 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	Full path of the backup filename. This entry must start with a slash (/) and must not contain a relative path.

Running a Backup Operation

SUMMARY STEPS

1. Choose **Administration > Operations >** *Backup-server* where *backup-server* is the server on which the backup file is stored.
2. In the General tab, enter the following information:
3. Click **Save**.
4. (Optional) To view the progress of the backup operation, click the **Task** tab. The Task tab provides the information described in the following table. The operation continues to run until it is completed.

DETAILED STEPS

Step 1 Choose **Administration > Operations >** *Backup-server* where *backup-server* is the server on which the backup file is stored.

Step 2 In the General tab, enter the following information:

a) In the Admin State field, choose **enabled**.

b) (Optional) Change the content of the other available fields.

Step 3 Click **Save**.
takes a snapshot of the configuration type that you selected and uploads the file to the network location.

Step 4 (Optional) To view the progress of the backup operation, click the **Task** tab. The Task tab provides the information described in the following table. The operation continues to run until it is completed.

Field	Description
Description	Task description.
Status	Task status.

Field	Description
Stage Descriptor	Description of the current stage.
Tries	Number of times the task has been tried.
Previous Status	Status of the previous task only. This field does not provide the status of the current task.
Remote Err Code	Remote error code.
Remote Err Description	Description of the remote error.
Remote Inv Result	Remote error result.
Time Stamp	Date and time when the task completed.
Progress	Progress of the current task, indicated by the percent complete, a progress bar, or both.

Editing a Backup Operation

Before You Begin

Obtain the backup server IP address or hostname and authentication credentials.

SUMMARY STEPS

1. Choose **Administration** > **Operations**.
2. Select the backup operation you want to edit, then click **Edit**.
3. In the Edit Backup dialog box, modify the information as required, then click **OK**.

DETAILED STEPS

Step 1 Choose **Administration** > **Operations**.

Step 2 Select the backup operation you want to edit, then click **Edit**.

Step 3 In the Edit Backup dialog box, modify the information as required, then click **OK**.

Field	Description
Admin State	One of the following administrative states: • enabled—Backup is enabled. The system runs the backup operation when you click **OK**. • disabled—Backup is disabled. The system does not run the backup operation when you click **OK**. If you choose this option, all fields in the dialog box remain visible.
Type	Backup type. The backup 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 system. This field is not editable.
Protocol	Protocol used when communicating with the remote server: • FTP • SCP • SFTP
Hostname/IP Address	Hostname or IP address of the device where the backup file is stored. This entry cannot be changed when editing the operation. If you use a hostname instead of an IP address, you must configure a DNS server.
User	Username the system uses to log into the remote server.
Password	Password the system uses to log into the remote server. This field is displayed if you choose **enabled** in the Admin State field. 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	Full path of the backup filename. This entry must start with a slash (/) and must not contain a relative path.

Deleting a Backup Operation

SUMMARY STEPS

1. Choose **Administration > Operations**.
2. Select the backup operation you want to delete, then click **Delete**.
3. When prompted, confirm the deletion.

DETAILED STEPS

Step 1 Choose **Administration > Operations**.

Step 2 Select the backup operation you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Restoring a Backup Configuration

SUMMARY STEPS

1. Install the virtual machine.
2. Uninstall the VSG policy agents. Connect the Secure Shell to the VSG console for this task. This step does not disrupt traffic.
3. Disable the ASA 1000V policy agent.
4. Uninstall the VSM policy agents. Connect the Secure Shell to the VSM console for this task. This step does not disrupt traffic.
5. Restore the database. Connect the Secure Shell to the CLI for this task. Depending upon your backup location, restore using FTP, SCP, or SFTP.
6. In the GUI, choose **Resource Management > Resources > VSMs**, and do the following:
7. In the GUI, choose **Resource Management > Resources > VSMs**, and verify that the deleted VSMs are not displayed.
8. Reregister the VSMs associated with by entering the following commands for each VSM:
9. Reinstall the VSM policy agents.
10. Wait until all the VSMs have registered with and are displayed under **Resource Management > Resources > VSMs**.
11. Reregister the VSGs associated with by entering the following commands for each VSG:
12. Reinstall the VSG policy agents.
13. Re-enable the ASA 1000V policy agent.
14. Verify the following states after the restore process is complete:

DETAILED STEPS

Step 1 Install the virtual machine.

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

Note Perform this step for all VSGs that are associated with the that you are restoring.

Example:

VMware
vsg# **conf t** vsg(config)# **vnmc-policy-agent** vsg(config-vnmc-policy-agent)# **no policy-agent-image**
Hyper-V Hypervisor
vsg# **conf t** vsg(config)# **nsc-policy-agent** vsg(config-nsc-policy-agent)# **no policy-agent-image**

Step 3 Disable the ASA 1000V policy agent.

Example:

VMware
asa# **conf t** asa(config)# **no vnmc policy-agent**
Hyper-V Hypervisor
Not available.

Step 4 Uninstall the VSM policy agents. Connect the Secure Shell to the VSM console for this task. This step does not disrupt traffic.

Note Perform this step for all VSMs that are associated with the you are restoring.

Example:

VMware

vsm# **conf t** vsm(config)# **vnmc-policy-agent** vsm(config-vnmc-policy-agent)# **no policy-agent-image**
Hyper-V Hypervisor
vsm# **conf t** vsm(config)# **nsc-policy-agent** vsm(config-nsc-policy-agent)# **no policy-agent-image**

Step 5 Restore the database. Connect the Secure Shell to the CLI for this task. Depending upon your backup location, restore using FTP, SCP, or SFTP.

Example:
nsc# **connect local-mgmt**

nsc(local-mgmt)# **restore scp://*username@server/path***

Step 6 In the GUI, choose **Resource Management > Resources > VSMs**, and do the following:

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

b) Choose each VSM, and click **Delete**.

Step 7 In the GUI, choose **Resource Management > Resources > VSMs**, and verify that the deleted VSMs are not displayed.

Step 8 Reregister the VSMs associated with by entering the following commands for each VSM:

Example:

VMware
vsm# **conf t** vsm(config)# **vnmc-policy-agent** vsm(config-vnmc-policy-agent)# **registration-ip *PrimeNSC-ip-address*** vsm(config-vnmc-policy-agent)# **shared-secret *password***
Hyper-V Hypervisor
vsm# **conf t** vsm(config)# **nsc-policy-agent** vms(config-nsc-policy-agent)# **registration-ip *PrimeNSC-ip-address*** vsm(config-nsc-policy-agent)# **shared-secret *password***

Step 9 Reinstall the VSM policy agents.

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

Example:

VMware
vsm# **conf t** vsm(config)# **vnmc-policy-agent** vsm(config-vnmc-policy-agent)# **policy-agent-image bootflash:nsc-vsmpa.*n.n.n*.bin**
Hyper-V Hypervisor
vsm# **conf t** vms(config)# **nsc-policy-agent** vsm(config-nsc-policy-agent)# **policy-agent-image bootflash:nsc-vsmpa.*n.n.n*.bin**

Step 10 Wait until all the VSMs have registered with and are displayed under **Resource Management > Resources > VSMs**.

Step 11 Reregister the VSGs associated with by entering the following commands for each VSG:

Example:

VMware
vsg# **conf t** vsg(config)# **vnmc-policy-agent** vsg(config-vnmc-policy-agent)# **registration-ip *PrimeNSC-ip-address*** vsg(config-vnmc-policy-agent)# **shared-secret *password***
Hyper-V Hypervisor
vsg# **conf t** vsg(config)# **nsc-policy-agent** vsg(config-nsc-policy-agent)# **registration-ip *PrimeNSC-ip-address*** vsg(config-nsc-policy-agent)# **shared-secret *password***

Step 12 Reinstall the VSG policy agents.

Note If the VSG policy agents must be upgraded, install the new software now.

Example:

VMware

vsg# **conf t** vsg(config)# **vnmc-policy-agent** vsg(config-vnmc-policy-agent)# **policy-agent-image bootflash:nsc-vsgpa.*n.n.n*.bin**
Hyper-V Hypervisor
vsg# **conf t** vsg(config)# **nsc-policy-agent** vsg(config-nsc-policy-agent)# **policy-agent-image bootflash:nsc-vsgpa.*n.n.n*.bin**

Step 13 Re-enable the ASA 1000V policy agent.

Example:

VMware
asa# **conf t** asa(config)# **vnmc policy-agent** asa(config-vnmc-policy-agent)# **shared-secret** ***password*** asa(config-vnmc-policy-agent)# **registration host** ***PrimeNSC-ip-address***
Hyper-V Hypervisor
Not available.

Step 14 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) Using the VSG CLI, verify that your configurations are restored to their earlier state.
b) Using the GUI, verify that your objects and policies are restored to their earlier state.
c) Using the ASA 1000V CLI, verify that your configurations are restored to their earlier state.

Managing Export Operations

Use export and import operations to migrate data from one server to another. To back up and restore data (for example, as a disaster recovery mechanism), use backup and restore operations.

Creating an Export Operation

The associations of compute and edge firewalls with VSGs and ASA 1000Vs, respectively, are not included in export or import data. Only firewall definitions are included, such as device profiles and policies. If an imported firewall did not exist in the system, it will not be associated to a VSG or ASA 1000V after the import operation. If an imported firewall already existed in the system, the association state remains the same.

Before You Begin

Obtain the remote file server IP address or hostname and authentication credentials before performing an export.

SUMMARY STEPS

1. Choose **Administration > Operations**.
2. Click **Create Export Operation**.
3. In the Create Export Operation dialog box, provide the required information as described in the following table, then click **OK**:

DETAILED STEPS

Step 1 Choose **Administration > Operations**.

Step 2 Click **Create Export Operation**.

Step 3 In the Create Export Operation dialog box, provide the required information as described in the following table, then click **OK**:

Field	Description
Admin State	One of the following administrative states: • enabled—Export is enabled. The system runs the export operation when you click **OK**. • disabled—Export is disabled. The system does not run the export operation when you click **OK**. If you choose this option, all fields in the dialog box remain visible.
Type	One of the following export types: • config-all • config-logical • config-system
Protocol	Protocol used when communicating with the remote server: • FTP • SCP • SFTP

Field	Description
Hostname/IP Address	Hostname or IP address of the device where the export file is stored. This entry cannot be changed when editing the operation. If you use a hostname instead of an IP address, you must configure a DNS server.
User	Username the system uses to log into the remote server.
Password	The password the system uses to log into the remote server. This field is displayed if you choose **enabled** in the Admin State field. does not store this password. You do not need to enter this password unless you intend to enable and run the export operation immediately.
Absolute Path Remote File (.tgz)	Full path of the .tgz filename. This entry must start with a slash (/) and must not contain a relative path.

Editing an Export Operation

Note The associations of compute and edge firewalls with VSGs and ASA 1000Vs, respectively, are not included in export or import data. Only firewall definitions are included, such as device profiles and policies. If an imported firewall did not exist in the system, it will not be associated to a VSG or ASA 1000V after the import operation. If an imported firewall already existed in the system, the association state remains the same.

Before You Begin

Obtain the remote file server IP address or hostname and authentication credentials before performing an export.

SUMMARY STEPS

1. Choose **Administration > Operations**.
2. In the Operations table, select the export operation you want to edit, then click **Edit**.
3. In the Edit Export dialog box, modify the fields as appropriate, then click **OK**.

DETAILED STEPS

Step 1 Choose **Administration > Operations**.

Step 2 In the Operations table, select the export operation you want to edit, then click **Edit**.

Step 3 In the Edit Export dialog box, modify the fields as appropriate, then click **OK**.

Field	Description
Admin State	One of the following administrative states: • enabled—Export is enabled. The system runs the export operation when you click **OK**. • disabled—Export is disabled. The system does not run the export operation when you click **OK**. If you choose this option, all fields in the dialog box remain visible.
Type	One of the following export types: • config-all • config-logical • config-system
Protocol	Protocol used when communicating with the remote server: • FTP • SCP • SFTP
Hostname/IP Address	Hostname or IP address of the device where the export file is stored. This entry cannot be changed when editing the operation. If you use a hostname instead of an IP address, you must configure a DNS server.
User	Username the system uses to log into the remote server.
Password	The password the system uses to log into the remote server. This field is displayed if you choose **enabled** in the Admin State field. does not store this password. You do not need to enter this password unless you intend to enable and run the export operation immediately.
Absolute Path Remote File (.tgz)	Full path of the .tgz filename. This entry must start with a slash (/) and must not contain a relative path.

Deleting an Export Operation

SUMMARY STEPS

1. In the Navigation pane, choose **Administration > Operations.**
2. In the Operations table, select the export operation you want to delete.
3. When prompted, confirm the deletion.

DETAILED STEPS

Step 1 In the Navigation pane, choose **Administration > Operations.**

Step 2 In the Operations table, select the export operation you want to delete.

Step 3 When prompted, confirm the deletion.

Configuring Import Operations

Creating an Import Operation

Before You Begin

Obtain the remote file server IP address or hostname and authentication credentials.

Note The association of compute and edge firewalls with VSGs and ASA 1000Vs, respectively, are not included in the export or import data. Only the compute and edge firewall definitions are included, such as device profiles and policies. Therefore, if an imported firewall did not exist in the system, it will not be associated to a VSG or ASA 1000V after the import operation. If an imported firewall already existed in the system, the association state remains the same.

Caution When the configuration data is imported into the server, you might see an error message and get logged out, followed by the display of a new certificate. This error occurs because the hostname, domain name, or both have changed. The VM Manager Extension needs to be exported again and installed on vCenter. To continue with the import, accept the certificate and log into again.

SUMMARY STEPS

1. Choose **Administration > Operations**.
2. Click **Create Import Operation**.
3. In the Create Import Operation dialog box, provide the following information as required, then click **OK**:

DETAILED STEPS

Step 1 Choose **Administration > Operations**.

Step 2 Click **Create Import Operation**.

Step 3 In the Create Import Operation dialog box, provide the following information as required, then click **OK**:

Field	Description
Admin State	One of the following administrative states: • enabled—Import is enabled. The system runs the import operation as soon as you click **OK**. • disabled—Import is disabled. The system does not run the import operation when you click **OK**. If you choose this option, all fields in the dialog box remain visible.
Action	Action to be taken on a file: merge.
Protocol	Protocol used when communicating with the remote server: • FTP • SCP • SFTP
Hostname/IP Address	Hostname or IP address of the device where the import file is stored. This entry cannot be changed when editing the operation. If you use a hostname instead of an IP address, you must configure a DNS server.
User	Username the system uses to log into the remote server. This field is displayed if you choose **enabled** in the Admin State field.
Password	Password the system uses to log into the remote server. does not store this password. You do not need to enter this password unless you intend to enable and run the import operation immediately.
Absolute Path Remote File (.tgz)	Full path of the .tgz filename. This entry must start with a slash (/) and must not contain a relative path.

Editing an Import Operation

Before You Begin

Obtain the remote file server IP address or hostname and authentication credentials.

SUMMARY STEPS

1. Choose **Administration > Operations**.
2. Select the import operation that you want to edit, then click **Edit**.
3. In the Edit dialog box, modify the fields as required, then click **OK**.

DETAILED STEPS

Step 1 Choose **Administration > Operations**.

Step 2 Select the import operation that you want to edit, then click **Edit**.

Step 3 In the Edit dialog box, modify the fields as required, then click **OK**.

Field	Description
Admin State	One of the following administrative states: • enabled—Import is enabled. The system runs the import operation as soon as you click **OK**. • disabled—Import is disabled. The system does not run the import operation when you click **OK**. If you choose this option, all fields in the dialog box remain visible.
Action	Action to be taken on a file: merge.
Protocol	Protocol used when communicating with the remote server: • FTP • SCP • SFTP
Hostname/IP Address	Hostname or IP address of the device where the import file is stored. This entry cannot be changed when editing the operation. If you use a hostname instead of an IP address, you must configure a DNS server.
User	Username the system uses to log into the remote server. This field is displayed if you choose **enabled** in the Admin State field.

Field	Description
Password	Password the system uses to log into the remote server. does not store this password. You do not need to enter this password unless you intend to enable and run the import operation immediately.
Absolute Path Remote File (.tgz)	Full path of the .tgz filename. This entry must start with a slash (/) and must not contain a relative path.

Deleting an Import Operation

SUMMARY STEPS

1. Choose **Administration > Operations**.
2. Select the import operation that you want to delete, then click **Delete**.
3. When prompted, confirm the deletion.

DETAILED STEPS

Step 1 Choose **Administration > Operations**.

Step 2 Select the import operation that you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.