Cisco Firepower 9300 FXOS Firepower Chassis Manager Configuration Guide, 1.1(3)

First Published: 2020-07-02

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

CONTENTS

CHAPTER 1

Introduction to the Firepower Security Appliance

About the Firepower Security Appliance

The Cisco Firepower 9300 chassis is a next-generation platform for network and content security solutions. The Firepower 9300 chassis is part of the Cisco Application Centric Infrastructure (ACI) Security Solution and provides an agile, open, secure platform that is built for scalability, consistent control, and simplified management.

The Firepower 9300 chassis provides the following features:

- Modular chassis-based security system—provides high performance, flexible input/output configurations, and scalability.
- Firepower Chassis Manager—graphical user interface provides streamlined, visual representation of current chassis status and simplified configuration of chassis features.
- FXOS CLI—provides command-based interface for configuring features, monitoring chassis status, and accessing advanced troubleshooting features.
- FXOS REST API—allows users to programmatically configure and manage their chassis.

Firepower Chassis Manager Overview

The Firepower eXtensible Operating System provides a web interface that makes it easy to configure platform settings and interfaces, provision devices, and monitor system status. The navigation bar at the top of the user interface provides access to the following:

- Overview—From the Overview page you can easily monitor the status of the Firepower chassis. For more information, see Monitoring the Chassis Status, on page 2.
- Interfaces—From the Interfaces page, you can view the status of the installed interfaces on the chassis, edit interface properties, enable or disable an interface, and create port channels. For more information, see Interface Management, on page 81.

- Logical Devices—From the Logical Devices page, you can create, edit, and delete logical devices. For more information, see Logical Devices, on page 89.
- Security Modules/Security Engine—From the Security Modules/Security Engine page, you can view the status of and can perform various functions on a security module/engine, such as power cycling, reinitializing, acknowledging, and decommissioning. For more information, see Security Module/Engine Management, on page 123.
- Platform Settings—From the Platform Settings page, you can configure chassis settings for the following: date and time, SSH, SNMP, HTTPS, AAA, Syslog, and DNS. For more information, see Platform Settings, on page 41.
- System Settings—From the System menu, you can manage the following settings:
    - Licensing—From the Licensing page, you can configure Smart Call Home settings and register your Firepower chassis with the Licensing Authority. For more information, see License Management for the ASA, on page 11.
    - Updates—From the Updates page, you can upload Platform Bundle and Application images to the Firepower chassis. For more information, see Image Management, on page 35.
    - User Management—From the User Management page you can configure user settings and define user accounts for the Firepower 9300 chassis. For more information, see User Management, on page 21.

Monitoring the Chassis Status

From the Overview page you can easily monitor the status of the Firepower 9300 chassis. The Overview page provides the following elements:

- Device Information—The top of the Overview page contains the following information about the Firepower 9300 chassis:
    - Chassis name—shows the name assigned to the chassis during initial configuration.
    - IP address—shows the management IP address assigned to the chassis during initial configuration.
    - Model—shows the Firepower 9300 chassis model.
    - Version—shows the FXOS version running on the chassis.
    - Operational State—shows the operable status for the chassis.
    - Chassis uptime—shows the elapsed time since the system was last restarted.

    Tip You can hover over the icon to the right of the Chassis uptime field to see uptime for a security module/engine.

- Visual Status Display—Below the Device Information section is a visual representation of the chassis that shows the components that are installed in the chassis and provides a general status for those components. You can hover over the ports that are shown in the Visual Status Display to get additional information such as interface name, speed, type, admin state, and operational state. For models with multiple security modules, you can hover over the security modules that are shown in the Visual Status Display to get additional information such as device name, template type, admin state, and operational state. If a logical device is installed on that security module, you can also see the management IP address, software version, and logical device mode.

- Detailed Status Information—Below the Visual Status Display is a table containing detailed status information for the chassis. The status information is broken up into five sections: Faults, Interfaces, Devices, License, and Inventory. You can see a summary for each of those sections above the table and you can see additional details for each of those sections by clicking on the summary area for the information you want to view.

  The system provides the following detailed status information for the chassis:

  - Faults—Lists the faults that have been generated in the system. The faults are sorted by severity: Critical, Major, Minor, Warning, and Info. For each fault that is listed, you can see the severity, a description of the fault, the cause, the number of occurrences, and the time of the most recent occurrence. You can also see whether the fault has been acknowledged or not.

    You can click on any of the faults to see additional details for the fault or to acknowledge the fault.

    Note Once the underlying cause of the fault has been addressed, the fault will automatically be cleared from the listing during the next polling interval. If a user is working on a resolution for a specific fault, they can acknowledge the fault to let other users know that the fault is currently being addressed.

  - Interfaces—Lists the interfaces installed in the system and shows the interface name, operational status, administrative status, number of received bytes, and number of transmitted bytes.
  - Devices—Lists the logical devices configured in the system and provides the following details for each logical device: device name, status, image version, management IP address.
  - License—(For ASA logical devices) Shows whether smart licensing is enabled, provides the current registration status of your Firepower license, and shows license authorization information for the chassis.
  - Inventory—Lists the components installed in the chassis and provides relevant details for those components, such as: component name, number of cores, installation location, operational status, operability, capacity, power, thermal, serial number, model number, part number, and vendor.

CHAPTER 2

Getting Started

Task Flow

The following procedure shows the basic tasks that should be completed when configuring your Firepower 9300 chassis.

Procedure

Step 1 Configure the Firepower 9300 chassis hardware (see the *Cisco Firepower Security Appliance Hardware Installation Guide*).

Step 2 Complete the initial configuration (see Initial Configuration Using Console Port, on page 5).

Step 3 Log in to the Firepower Chassis Manager (see Log In or Out of the Firepower Chassis Manager, on page 8).

Step 4 Set the Date and Time (see Setting the Date and Time, on page 43).

Step 5 Configure a DNS server (see Configuring DNS Servers, on page 78).

Step 6 Register your product license (see License Management for the ASA, on page 11).

Step 7 Configure users (see User Management, on page 21).

Step 8 Perform software updates as required (see Image Management, on page 35).

Step 9 Configure additional platform settings (see Platform Settings, on page 41).

Step 10 Configure interfaces (see Interface Management, on page 81).

Step 11 Create logical devices (see Logical Devices, on page 89).

Initial Configuration Using Console Port

Before you can use Firepower Chassis Manager or the FXOS CLI to configure and manage your system, you must perform some initial configuration tasks using the FXOS CLI accessed through the console port.Use the following procedure to perform initial configuration using the FXOS CLI accessed through the console port. The first time that you access the Firepower 9300 chassis using the FXOS CLI, you will encounter a setup wizard that you can use to configure the system.

Note To repeat the initial setup, you need to erase any existing configuration using the following commands:

```
Firepower-chassis# connect local-mgmt
firepower-chassis(local-mgmt)# erase configuration
```

You can choose to either restore the system configuration from an existing backup file, or manually set up the system by going through the Setup wizard. If you choose to restore the system, the backup file must be reachable from the management network.

You must specify only one IPv4 address, gateway, and subnet mask, or only one IPv6 address, gateway, and network prefix for the single management port on the Firepower 9300 chassis. You can configure either an IPv4 or an IPv6 address for the management port IP address.

Before you begin

1. Verify the following physical connections on the Firepower 9300 chassis:
    - The console port is physically connected to a computer terminal or console server.
    - The 1 Gbps Ethernet management port is connected to an external hub, switch, or router.

    For more information, refer to the *Cisco Firepower Security Appliance Hardware Installation Guide*.
2. Verify that the console port parameters on the computer terminal (or console server) attached to the console port are as follows:
    - 9600 baud
    - 8 data bits
    - No parity
    - 1 stop bit
3. Gather the following information for use with the setup script:
    - New admin password
    - Management IP address and subnet mask
    - Gateway IP address
    - Hostname and domain name
    - DNS server IP address

Procedure

Step 1 Power on the chassis.

Step 2 Connect to the serial console port using a terminal emulator.

The Firepower includes an RS-232–to–RJ-45 serial console cable. You might need to use a third party serial-to-USB cable to make the connection. Use the following serial parameters:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit

Step 3 Complete the system configuration as prompted.

Example:

```
Enter the setup mode; setup newly or restore from backup. (setup/restore) ? setup
You have chosen to setup a new Fabric interconnect. Continue? (y/n): y
Enforce strong password? (yes/no) [y]: n
Enter the password for "admin": Farscape&32
Confirm the password for "admin": Farscape&32
Enter the system name:  firepower-9300
Physical Switch Mgmt0 IP address : 10.80.6.12
Physical Switch Mgmt0 IPv4 netmask : 255.255.255.0
IPv4 address of the default gateway : 10.80.6.1
Configure the DNS Server IP address? (yes/no) [n]: y
  DNS IP address : 10.164.47.13
Configure the default domain name? (yes/no) [n]: y
  Default domain name : cisco.com

Following configurations will be applied:
  Switch Fabric=A
  System Name=firepower-9300
  Enforced Strong Password=no
  Physical Switch Mgmt0 IP Address=10.89.5.14
  Physical Switch Mgmt0 IP Netmask=255.255.255.192
  Default Gateway=10.89.5.1
  IPv6 value=0
  DNS Server=72.163.47.11
  Domain Name=cisco.com

Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): y
Applying configuration. Please wait...  Configuration file - Ok
.....

Cisco FPR Series Security Appliance
firepower-9300 login:  admin
Password: Farscape&32
Successful login attempts for user 'admin' : 1
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2019, Cisco Systems, Inc. All rights reserved.

[...]
```

```
firepower-chassis#
```

Log In or Out of the Firepower Chassis Manager

Before you can configure your Firepower 9300 chassis using Firepower Chassis Manager, you must log in using a valid user account. For more information on user accounts, see User Management, on page 21.

You are automatically logged out of the system if a certain period of time passes without any activity. By default, the system will log you out after 10 minutes of inactivity. To configure this timeout setting, see Configuring the Session Timeout, on page 29.

Note You can optionally configure your Firepower Chassis Manager to allow only a certain number of unsuccessful login attempts before the user is locked out of the system for a specified amount of time. For more information, see Set the Maximum Number of Login Attempts, on page 30.

Procedure

Step 1 To log in to the Firepower Chassis Manager:

a) Using a supported browser, enter the following URL in the address bar:

https://*<chassis_mgmt_ip_address>*

where <*chassis_mgmt_ip_address*> is the IP address or host name of the Firepower 9300 chassis that you entered during initial configuration.

Note For information on supported browsers, refer to the release notes for the version you are using (see http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list.html).

b) Enter your username and password.

c) Click **Login**.

You are logged in and the Firepower Chassis Manager opens to show the Overview page.

Step 2 To log out of the Firepower Chassis Manager, point at your username in the navigation bar and then select **Logout**.

You are logged out of the Firepower Chassis Manager and are returned to the login screen.

Accessing the FXOS CLI

You can connect to the FXOS CLI using a terminal plugged into the console port. Verify that the console port parameters on the computer terminal (or console server) attached to the console port are as follows:

- 9600 baud

- 8 data bits
- No parity
- 1 stop bit

You can also connect to the FXOS CLI using SSH and Telnet. The Firepower eXtensible Operating System supports up to eight simultaneous SSH connections. To connect with SSH, you need to know the hostname or IP address of the Firepower 9300 chassis.

Use one of the following syntax examples to log in with SSH, Telnet, or Putty:

Note SSH log in is case-sensitive.

From a Linux terminal using SSH:

- **ssh ucs-***auth-domain**username*@{*UCSM-ip-address* | *UCMS-ipv6-address*}

```
ssh ucs-example\\jsmith@192.0.20.11
```

```
ssh ucs-example\\jsmith@2001::1
```

- **ssh -l ucs-***auth-domain**username* {*UCSM-ip-address*| *UCSM-ipv6-address*| *UCSM-host-name*}

```
ssh -l ucs-example\\jsmith 192.0.20.11
```

```
ssh -l ucs-example\\jsmith 2001::1
```

- **ssh** {*UCSM-ip-address* | *UCSM-ipv6-address* | *UCSM-host-name*} **-l ucs-***auth-domain**username*

```
ssh 192.0.20.11 -l ucs-example\\jsmith
```

```
ssh 2001::1 -l ucs-example\\jsmith
```

- **ssh ucs-***auth-domain**username*@{*UCSM-ip-address* | *UCSM-ipv6-address*}

```
ssh ucs-ldap23\\jsmith@192.0.20.11
```

```
ssh ucs-ldap23\\jsmith@2001::1
```

From a Linux terminal using Telnet:

Note Telnet is disabled by default. See Configuring Telnet, on page 45 for instructions on enabling Telnet.

- **telnet ucs-***UCSM-host-name* **ucs-***auth-domain**username*

```
telnet ucs-qa-10
login: ucs-ldap23\blradmin
```

- **telnet ucs-**{*UCSM-ip-address* | *UCSM-ipv6-address*}*ucs-auth-domain**username*

```
telnet 10.106.19.12 2052
ucs-qa-10-A login: ucs-ldap23\blradmin
```

From a Putty client:

- Login as: **ucs-***auth-domain**username*

```
Login as: ucs-example\jsmith
```

Note If the default authentication is set to local, and the console authentication is set to LDAP, you can log in to the fabric interconnect from a Putty client using **`ucs-local\admin`**, where admin is the name of the local account.

CHAPTER 3

License Management for the ASA

Cisco Smart Software Licensing lets you purchase and manage a pool of licenses centrally. You can easily deploy or retire devices without having to manage each unit's license key. Smart Software Licensing also lets you see your license usage and needs at a glance.

> **Note** This section only applies to ASA logical devices on the Firepower 9300 chassis. For more information on licensing for Firepower Threat Defense logical devices, see the Firepower Management Center Configuration Guide.

About Smart Software Licensing

This section describes how Smart Software Licensing works.

> **Note** This section only applies to ASA logical devices on the Firepower 9300 chassis. For more information on licensing for Firepower Threat Defense logical devices, see the Firepower Management Center Configuration Guide.

Smart Software Licensing for the ASA

For the ASA application on the Firepower 9300 chassis, Smart Software Licensing configuration is split between the Firepower 9300 chassis supervisor and the application.

- Firepower 9300 chassis—Configure all Smart Software Licensing infrastructure in the supervisor, including parameters for communicating with the License Authority. The Firepower 9300 chassis itself does not require any licenses to operate.
- ASA Application—Configure all license entitlements in the application.

Note Cisco Transport Gateway is not supported on Firepower 4100/9300 security appliances.

Smart Software Manager and Accounts

When you purchase 1 or more licenses for the device, you manage them in the Cisco Smart Software Manager:

https://software.cisco.com/#module/SmartLicensing

The Smart Software Manager lets you create a master account for your organization.

Note If you do not yet have an account, click the link to set up a new account. The Smart Software Manager lets you create a master account for your organization.

By default, your licenses are assigned to the *Default Virtual Account* under your master account. As the account administrator, you can optionally create additional virtual accounts; for example, you can create accounts for regions, departments, or subsidiaries. Multiple virtual accounts let you more easily manage large numbers of licenses and devices.

Offline Management

If your devices do not have Internet access, and cannot register with the License Authority, you can configure offline licensing.

Satellite Server

If your devices cannot access the internet for security reasons, you can optionally install a local Smart Software Manager satellite server as a virtual machine (VM). The satellite provides a subset of Smart Software Manager functionality, and allows you to provide essential licensing services for all your local devices. Only the satellite needs to connect periodically to the main License Authority to sync your license usage. You can sync on a schedule or you can sync manually.

Once you download and deploy the satellite application, you can perform the following functions without sending data to Cisco SSM using the Internet:

- Activate or register a license
- View your company's licenses
- Transfer licenses between company entities

For more information, see the Smart Software Manager satellite installation and configuration guides on Smart Account Manager satellite.

Licenses and Devices Managed per Virtual Account

Licenses and devices are managed per virtual account: only that virtual account's devices can use the licenses assigned to the account. If you need additional licenses, you can transfer an unused license from another virtual account. You can also transfer devices between virtual accounts.

Only the Firepower 9300 chassis registers as a device, while the ASA applications in the chassis request their own licenses. For example, for a Firepower 9300 chassis with 3 security modules, the chassis counts as one device, but the modules use 3 separate licenses.

Evaluation License

The Firepower 9300 chassis supports two types of evaluation license:

- Chassis-level evaluation mode—Before the Firepower 9300 chassis registers with the Licensing Authority, it operates for 90 days (total usage) in evaluation mode. The ASA cannot request specific entitlements in this mode; only default entitlements are enabled. When this period ends, the Firepower 9300 chassis becomes out-of-compliance.
- Entitlement-based evaluation mode—After the Firepower 9300 chassis registers with the Licensing Authority, you can obtain time-based evaluation licenses that can be assigned to the ASA. In the ASA, you request entitlements as usual. When the time-based license expires, you need to either renew the time-based license or obtain a permanent license.

Note You cannot receive an evaluation license for Strong Encryption (3DES/AES); only permanent licenses support this entitlement.

Smart Software Manager Communication

This section describes how your device communicates with the Smart Software Manager.

Device Registration and Tokens

For each virtual account, you can create a registration token. This token is valid for 30 days by default. Enter this token ID plus entitlement levels when you deploy each chassis, or when you register an existing chassis. You can create a new token if an existing token is expired.

At startup after deployment, or after you manually configure these parameters on an existing chassis, the chassis registers with the Cisco License Authority. When the chassis registers with the token, the License Authority issues an ID certificate for communication between the chassis and the License Authority. This certificate is valid for 1 year, although it will be renewed every 6 months.

Periodic Communication with the License Authority

The device communicates with the License Authority every 30 days. If you make changes in the Smart Software Manager, you can refresh the authorization on the device so the change takes place immediately. Or you can wait for the device to communicate as scheduled.

You can optionally configure an HTTP proxy.

The Firepower 9300 chassis must have internet access either directly or through an HTTP proxy at least every 90 days. Normal license communication occurs every 30 days, but with the grace period, your device will operate for up to 90 days without calling home. After the grace period, you must contact the Licensing Authority, or you will not be able to make configuration changes to features requiring special licenses; operation is otherwise unaffected.

Note If your device is unable to communicate with the license authority for one year, the device will enter an unregistered state without strong encryption licenses.

Out-of-Compliance State

The device can become out of compliance in the following situations:

- Over-utilization—When the device uses unavailable licenses.
- License expiration—When a time-based license expires.
- Lack of communication—When the device cannot reach the Licensing Authority for re-authorization.

To verify whether your account is in, or approaching, an Out-of-Compliance state, you must compare the entitlements currently in use by your Firepower 9300 chassis against those in your Smart Account.

In an out-of-compliance state, you will not be able to make configuration changes to features requiring special licenses, but operation is otherwise unaffected. For example, existing contexts over the Standard license limit can continue to run, and you can modify their configuration, but you will not be able to add a *new* context.

Smart Call Home Infrastructure

By default, a Smart Call Home profile exists in the FXOS configuration that specifies the URL for the Licensing Authority. You cannot remove this profile. Note that the only configurable option for the License profile is the destination address URL for the License Authority. Unless directed by Cisco TAC, you should not change the License Authority URL.

Note Cisco Transport Gateway is not supported on Firepower 4100/9300 security appliances.

Prerequisites for Smart Software Licensing

- Note that this chapter only applies to ASA logical devices on the Firepower 9300 chassis. For more information on licensing for Firepower Threat Defense logical devices, see the Firepower Management Center Configuration Guide.
- Create a master account on the Cisco Smart Software Manager:

  https://software.cisco.com/#module/SmartLicensing

  If you do not yet have an account, click the link to set up a new account. The Smart Software Manager lets you create a master account for your organization.

- Purchase 1 or more licenses from the Cisco Commerce Workspace. On the home page, search for your platform in the **Find Products and Solutions** search field. Some licenses are free, but you still need to add them to your Smart Software Licensing account.
- Ensure internet access or HTTP proxy access from the chassis, so the chassis can contact the Licensing Authority.
- Configure a DNS server so the chassis can resolve the name of the Licensing Authority.
- Set the time for the chassis.
- Configure the Smart Software Licensing infrastructure on the Firepower 9300 chassis before you configure the ASA licensing entitlements.

Guidelines for Smart Software Licensing

ASA Guidelines for Failover and Clustering

Each Firepower 9300 chassis must be registered with the License Authority or satellite server. There is no extra cost for secondary units.

Defaults for Smart Software Licensing

The Firepower 9300 chassis default configuration includes a Smart Call Home profile called “SLProfile” that specifies the URL for the Licensing Authority.

Configure Regular Smart Software Licensing

To communicate with the Cisco License Authority, you can optionally configure an HTTP proxy. To register with the License Authority, you must enter the registration token ID on the Firepower 9300 chassis that you obtained from your Smart Software License account.

Procedure

Step 1 (Optional) Configure the HTTP Proxy, on page 15.

Step 2 Register the Firepower Security Appliance with the License Authority, on page 16.

(Optional) Configure the HTTP Proxy

If your network uses an HTTP proxy for Internet access, you must configure the proxy address for Smart Software Licensing. This proxy is also used for Smart Call Home in general.

Note HTTP proxy with authentication is not supported.

Procedure

Step 1 Choose **System** > **Licensing** > **Call Home**.

The Call Home page provides fields for configuring the destination address URL for the License Authority and for configuring an HTTP proxy.

Note Unless directed by Cisco TAC, you should not change the License Authority URL.

Step 2 In the Server Enable drop-down list, select **on**.

Step 3 Enter the proxy IP address and port in the **Server URL** and **Server Port** fields. For example, enter port 443 for an HTTPS server.

Step 4 Click **Save**.

Register the Firepower Security Appliance with the License Authority

When you register the Firepower 9300 chassis, the License Authority issues an ID certificate for communication between the Firepower 9300 chassis and the License Authority. It also assigns the Firepower 9300 chassis to the appropriate virtual account. Normally, this procedure is a one-time instance. However, you might need to later re-register the Firepower 9300 chassis if the ID certificate expires because of a communication problem, for example.

Procedure

Step 1 In the Smart Software Manager or the Smart Software Manager Satellite, request and copy a registration token for the virtual account to which you want to add this Firepower 9300 chassis.

For more information on how to request a registration token using the Smart Software Manager Satellite, see the Cisco Smart Software Manager Satellite User Guide (https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html).

Step 2 In Firepower Chassis Manager, choose **System** > **Licensing** > **Smart License**.

Step 3 Enter the registration token in the **Enter Product Instance Registration Token** field.

Step 4 Click **Register**.

The Firepower 9300 chassis attempts to register with the License Authority.

To unregister the device, click **Unregister**.

Deregistering the Firepower 9300 chassis removes the device from your account. All license entitlements and certificates on the device are removed. You might want to deregister to free up a license for a new Firepower 9300 chassis. Alternatively, you can remove the device from the Smart Software Manager.

Change Cisco Success Network Enrollment

You enable Cisco Success Network when you register the Firepower 9300 with the Cisco Smart Software Manager. After that, use the following procedure to view or change enrollment status.

Note Cisco Success Network does not work in evaluation mode.

Procedure

Step 1 Choose **System** > **Licensing** > **Cisco Success Network**.

Step 2 Under **Cisco Success Network Preferences**, read the information provided by Cisco, and click **Click here** to check out the sample data that will be sent to Cisco.

Step 3 Choose whether you want to **Enable Cisco Success Network**, and click **Save**.

Configure a Smart License Satellite Server for the Firepower 9300 chassis

The following procedure shows how to configure the Firepower 9300 chassis to use a Smart License satellite server.

Before you begin

- Complete all prerequisites listed in the Prerequisites for Smart Software Licensing, on page 14.
- Deploy and set up a Smart Software Satellite Server:

  Download the Smart License Satellite OVA file from Cisco.com and install and configure it on a VMwareESXi server. For more information, see the Smart Software Manager satellite Install Guide.
- Verify that the FQDN of the Smart Software Satellite Server can be resolved by your internal DNSserver.
- Verify whether the satellite trustpoint is already present:

  scope security

  show trustpoint

  Note that the trustpoint is added by default in FXOS version 2.4(1) and later. If the trustpoint is not present, you must add one manually using the following steps:

  1. Go to http://www.cisco.com/security/pki/certs/clrca.cer and copy the entire body of the SSL certificate (from "-----BEGIN CERTIFICATE-----" to "-----END CERTIFICATE-----") into a place you can access during configuration.
  2. Enter security mode:

     scope security

3. Create and name a trusted point:

   create trustpoint *trustpoint_name*

4. Specify certificate information for the trust point. Note: the certificate must be in Base64 encoded X.509 (CER) format.

   set certchain *certchain*

   For the *certchain* variable, paste the certificate text that you copied in step 1.

   If you do not specify certificate information in the command, you are prompted to enter a certificate or a list of trust points defining a certification path to the root certificate authority (CA). On the next line following your input, type **ENDOFBUF** to finish.

5. Commit the configuration:

   commit-buffer

Procedure

Step 1 Choose **System** > **Licensing** > **Call Home**.

Step 2 In the **Call home Configuration** area, replace the default URL in the **Address** field with the URL of your Smart Software Satellite Server using information that you gathered in the prerequisites for this procedure, using the following format: **https://***[FQDN of Satellite server]***/Transportgateway/services/DeviceRequestHandler**

Step 3 Register the Firepower Security Appliance with the License Authority, on page 16. Note that you must request and copy the registration token from the Smart License Manager satellite.

History for Smart Software Licensing

Feature Name	Platform Releases	Description
Cisco Success Network	2.7.1	Cisco Success Network is a user-enabled cloud service. When you enable Cisco Success Network, a secure connection is established between the Firepower 9300 chassis and the Cisco cloud to stream usage information and statistics. Streaming telemetry provides a mechanism that selects data of interest from the ASA and transmits it in a structured format to remote management stations to do the following: • Inform you of available unused features that can improve the effectiveness of the product in your network • Inform you of additional technical support services and monitoring that might be available for your product • Help Cisco improve our products Once you enroll in the Cisco Success Network, the chassis establishes and maintains the secure connection at all times. You can turn off this connection at any time by disabling Cisco Success Network, which disconnects the device from the Cisco Success Network cloud. We introduced the following commands: **scope telemetry {enable | disable}** We introduced the following screens: **System** > **Licensing** > **Cisco Success Network**

Feature Name	Platform Releases	Description
Cisco Smart Software Licensing for the Firepower 9300 chassis	1.1(1)	Smart Software Licensing lets you purchase and manage a pool of licenses. Smart licenses are not tied to a specific serial number. You can easily deploy or retire devices without having to manage each unit's license key. Smart Software Licensing also lets you see your license usage and needs at a glance. Smart Software Licensing configuration is split between the Firepower 9300 chassis supervisor and the security module. We introduced the following screens: **System** > **Licensing** > **Call Home** **System** > **Licensing** > **Smart License**

CHAPTER 4

User Management

User Accounts

User accounts are used to access the system. You can configure up to 48 local user accounts. Each user account must have a unique username and password.

Admin Account

The admin account is a default user account and 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.

The admin account is always active and does not expire. You cannot configure the admin account as inactive.

Locally Authenticated User Accounts

A locally authenticated user account is authenticated directly through the chassis and can be enabled or disabled by anyone with admin or AAA privileges. Once a local user account is disabled, the user cannot log in. Configuration details for disabled local user accounts are not deleted by the database. If you reenable a disabled local user account, the account becomes active again with the existing configuration; however, the account password must be reset.

Remotely Authenticated User Accounts

A remotely authenticated user account is any user account that is authenticated through LDAP, RADIUS, or TACACS+.

If a user maintains a local user account and a remote user account simultaneously, the roles defined in the local user account override those maintained in the remote user account.

See the following topics for more information on guidelines for remote authentication, and how to configure and delete remote authentication providers:

- Guidelines for Remote Authentication, on page 23
- Configuring LDAP Providers, on page 68
- Configuring RADIUS Providers, on page 72
- Configuring TACACS+ Providers, on page 74

Expiration of User Accounts

You can configure user accounts to expire at a predefined time. When the expiration time is reached, the user account is disabled.

By default, user accounts do not expire.

After you configure a user account with an expiration date, you cannot reconfigure the account to not expire. You can, however, configure the account with the latest expiration date available.

Guidelines for Usernames

The username is also used as the login ID for Firepower Chassis Manager and the FXOS CLI. When you assign login IDs to user accounts, consider the following guidelines and restrictions:

- The login ID can contain between 1 and 32 characters, including the following:
  - Any alphabetic character
  - Any digit
  - _ (underscore)
  - - (dash)
  - . (dot)
- The login ID must be unique.
- The login ID must start with an alphabetic character. It cannot start with a number or a special character, such as an underscore.
- The login ID is case-sensitive.
- You cannot create an all-numeric login ID.
- After you create a user account, you cannot change the login ID. You must delete the user account and create a new one.

Guidelines for Passwords

A password is required for each locally authenticated user account. A user with admin or AAA privileges can configure the system to perform a password strength check on user passwords. If the password strength check is enabled, each user must have a strong password.

We recommend that each user have a strong password. If you enable the password strength check for locally authenticated users, the Firepower eXtensible Operating System rejects any password that does not meet the following requirements:

- Must contain a minimum of 8 characters and a maximum of 80 characters.
- Must contain at least three of the following:
    - An uppercase alphabetic character
    - A lowercase alphabetic character
    - A non-alphanumeric (special) character
    - Digits
- Must not contain a space.
- Must not contain a character that is repeated more than 3 times consecutively, such as aaabbb.
- Must not contain three consecutive numbers or letters in any order, such as passwordABC or password321.
- Must not be identical to the username or the reverse of the username.
- Must pass a password dictionary check. For example, the password must not be based on a standard dictionary word.
- Must not contain the following symbols: $ (dollar sign), ? (question mark), and = (equals sign).

    Note This restriction applies whether the password strength check is enabled or not.

- Must not be blank for local user and admin accounts.

Guidelines for Remote Authentication

If a system is configured for one of the supported remote authentication services, you must create a provider for that service to ensure that the Firepower 9300 chassis can communicate with the system. The following guidelines impact user authorization:

User Accounts in Remote Authentication Services

User accounts can exist locally in the Firepower 9300 chassis or in the remote authentication server.

You can view the temporary sessions for users who log in through remote authentication services from the Firepower Chassis Manager or the FXOS CLI.

User Roles in Remote Authentication Services

If you create user accounts in the remote authentication server, you must ensure that the accounts include the roles those users require for working in the Firepower 9300 chassis and that the names of those roles match the names used in FXOS. Based on the role policy, a user might not be allowed to log in, or is granted only read-only privileges.

User Attributes in Remote Authentication Providers

For RADIUS and TACACS+ configurations, you must configure a user attribute for the Firepower 9300 chassis in each remote authentication provider through which users log in to Firepower Chassis Manager or the FXOS CLI. This user attribute holds the roles and locales assigned to each user.

When a user logs in, FXOS does the following:

1. Queries the remote authentication service.
2. Validates the user.
3. If the user is validated, checks the roles and locales assigned to that user.

The following table contains a comparison of the user attribute requirements for the remote authentication providers supported by FXOS:

Authenication Provider	Custom Attribute	Schema Extension	Attribute ID Requirements
LDAP	Optional	You can choose to do one of the following: • Do not extend the LDAP schema and configure an existing, unused attribute that meets the requirements. • Extend the LDAP schema and create a custom attribute with a unique name, such as CiscoAVPair.	The Cisco LDAP implementation requires a unicode type attribute. If you choose to create the CiscoAVPair custom attribute, use the following attribute ID: 1.3.6.1.4.1.9.287247.1 A sample OID is provided in the following section.
RADIUS	Optional	You can choose to do one of the following: • Do not extend the RADIUS schema and use an existing, unused attribute that meets the requirements. • Extend the RADIUS schema and create a custom attribute with a unique name, such as cisco-avpair.	The vendor ID for the Cisco RADIUS implementation is 009 and the vendor ID for the attribute is 001. The following syntax example shows how to specify multiples user roles and locales if you choose to create the cisco-avpair attribute: `shell:roles="admin,aaa" shell:locales="L1,abc"`. Use a comma "," as the delimiter to separate multiple values.

Authenication Provider	Custom Attribute	Schema Extension	Attribute ID Requirements
TACACS+	Required	You must extend the schema and create a custom attribute with the name cisco-av-pair.	The cisco-av-pair name is the string that provides the attribute ID for the TACACS+ provider. The following syntax example shows how to specify multiples user roles and locales when you create the cisco-av-pair attribute: `cisco-av-pair=shell:roles="admin aaa" shell:locales*"L1 abc"`. Using an asterisk (*) in the cisco-av-pair attribute syntax flags the locale as optional, preventing authentication failures for other Cisco devices that use the same authorization profile. Use a space as the delimiter to separate multiple values.

Sample OID for LDAP User Attribute

The following is a sample OID for a custom CiscoAVPair attribute:

```
CN=CiscoAVPair,CN=Schema,
CN=Configuration,CN=X
objectClass: top
objectClass: attributeSchema
cn: CiscoAVPair
distinguishedName: CN=CiscoAVPair,CN=Schema,CN=Configuration,CN=X
instanceType: 0x4
uSNCreated: 26318654
attributeID: 1.3.6.1.4.1.9.287247.1
attributeSyntax: 2.5.5.12
isSingleValued: TRUE
showInAdvancedViewOnly: TRUE
adminDisplayName: CiscoAVPair
adminDescription: UCS User Authorization Field
oMSyntax: 64
lDAPDisplayName: CiscoAVPair
name: CiscoAVPair
objectCategory: CN=Attribute-Schema,CN=Schema,CN=Configuration,CN=X
```

User Roles

The system contains the following user roles:

Administrator

Complete read-and-write access to the entire system. The default admin account is assigned this role by default and it cannot be changed.

Read-Only

Read-only access to system configuration with no privileges to modify the system state.

Password Profile for Locally Authenticated Users

The password profile contains the password history and password change interval properties for all locally authenticated users. You cannot specify a different password profile for each locally authenticated user.

Password History Count

The password history count allows you to prevent locally authenticated users from reusing the same password over and over again. When this property is configured, the Firepower chassis stores passwords that were previously used by locally authenticated users up to a maximum of 15 passwords. The passwords are stored in reverse chronological order with the most recent password first to ensure that the only the oldest password can be reused when the history count threshold is reached.

A user must create and use the number of passwords configured in the password history count before being able to reuse one. For example, if you set the password history count to 8, a locally authenticated user cannot reuse the first password until after the ninth password has expired.

By default, the password history is set to 0. This value disables the history count and allows users to reuse previously passwords at any time.

If necessary, you can clear the password history count for a locally authenticated user and enable reuse of previous passwords.

Password Change Interval

The password change interval enables you to restrict the number of password changes a locally authenticated user can make within a given number of hours. The following table describes the two configuration options for the password change interval.

Interval Configuration	Description	Example
No password change allowed	This option does not allow passwords for locally authenticated users to be changed within a specified number of hours after a password change. You can specify a no change interval between 1 and 745 hours. By default, the no change interval is 24 hours.	For example, to prevent passwords from being changed within 48 hours after a locally authenticated user changes his or her password, set the following: • Change during interval to disable • No change interval to 48

Interval Configuration	Description	Example
Password changes allowed within change interval	This option specifies the maximum number of times that passwords for locally authenticated users can be changed within a pre-defined interval. You can specify a change interval between 1 and 745 hours and a maximum number of password changes between 0 and 10. By default, a locally authenticated user is permitted a maximum of 2 password changes within a 48 hour interval.	For example, to allow a password to be changed a maximum of once within 24 hours after a locally authenticated user changes his or her password, set the following: • Change during interval to enable • Change count to 1 • Change interval to 24

Configuring User Settings

Procedure

Step 1 Choose **System** > **User Management**.

Step 2 Click the **Settings** tab.

Step 3 Complete the following fields with the required information:

Note If **Default Authentication** and **Console Authentication** are both set to use the same remote authentication protocol (RADIUS, TACACS+, or LDAP), you cannot change certain aspects of that server's configuration (for example, deleting that server, or changing its order of assignment) without updating these user settings.

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Default Authentication field</td><td>The default method by which a user is authenticated during remote login. This can be one of the following:
• Local—The user account must be defined locally on the Firepower chassis.
• Radius—The user account must be defined on the RADIUS server specified for the Firepower chassis.
• TACACS—The user account must be defined on the TACACS+ server specified for the Firepower chassis.
• LDAP—The user account must be defined on the LDAP/MS-AD server specified for the Firepower chassis.
• None—If the user account is local to the Firepower chassis, no password is required when the user logs in remotely.
Note All Radius, TACACS, and LDAP settings must be configured under Platform Settings. For more information, see About AAA, on page 66 in the Platform Settings chapter.</td></tr>
<tr><td colspan="2">Remote User Settings</td></tr>
<tr><td>Remote User Role Policy</td><td>Controls what happens when a user attempts to log in and the remote authentication provider does not supply a user role with the authentication information:
• Assign Default Role—The user is allowed to log in with a read-only user role.
• No-Login—The user is not allowed to log in to the system, even if the username and password are correct.</td></tr>
<tr><td colspan="2">Local User Settings</td></tr>
<tr><td>Password Strength Check check box</td><td>If checked, all local user passwords must conform to the guidelines for a strong password (see Guidelines for Passwords, on page 23).</td></tr>
<tr><td>History Count field</td><td>The number of unique passwords a user must create before the user can reuse a previously used password. The history count is in reverse chronological order with the most recent password first to ensure that only the oldest password can be reused when the history count threshold is reached.
This value can be anywhere from 0 to 15.
You can set the History Count field to 0 to disable the history count and allow users to reuse previously used passwords at any time.</td></tr>
</table>

Name	Description
Change During Interval field	Controls when a locally authenticated user can change his or her password. This can be: • **Enable**—Locally authenticated users can change their passwords based on the settings for Change Interval and Change Count. • **Disable**—Locally authenticated users cannot change their passwords for the period of time specified for No Change Interval.
Change Interval field	The number of hours over which the number of password changes specified in the **Change Count** field are enforced. This value can be anywhere from 1 to 745 hours. For example, if this field is set to 48 and the **Change Count** field is set to 2, a locally authenticated user can make no more than 2 password changes within a 48 hour period.
Change Count field	The maximum number of times a locally authenticated user can change his or her password during the Change Interval. This value can be anywhere from 0 to 10.
No Change Interval field	The minimum number of hours that a locally authenticated user must wait before changing a newly created password. This value can be anywhere from 1 to 745 hours. This interval is ignored if the **Change During Interval** property is not set to **Disable**.

Step 4 Click **Save**.

Configuring the Session Timeout

You can use the FXOS CLI to specify the amount of time that can pass without user activity before the Firepower 9300 chassis closes user sessions. You can configure different settings for console sessions and for HTTPS, SSH, and Telnet sessions.

You can set a timeout value up to 3600 seconds (60 minutes). The default value is 600 seconds. To disable this setting, set the session timeout value to 0.

Procedure

Step 1 Enter security mode:

Firepower-chassis # **scope security**

Step 2 Enter default authorization security mode:

Firepower-chassis /security # **scope default-auth**

Step 3 Set the idle timeout for HTTPS, SSH, and Telnet sessions:

Firepower-chassis /security/default-auth # **set session-timeout** *seconds*

Step 4 (Optional) Set the idle timeout for console sessions:

Firepower-chassis /security/default-auth # **set con-session-timeout** *seconds*

Step 5 Commit the transaction to the system configuration:

Firepower-chassis /security/default-auth # **commit-buffer**

Step 6 (Optional) View the session and absolute session timeout settings:

Firepower-chassis /security/default-auth # **show detail**

Example:

```
Default authentication:
 Admin Realm: Local
 Operational Realm: Local
 Web session refresh period(in secs): 600
 Idle Session timeout (in secs) for web, ssh, telnet sessions: 600
 Absolute Session timeout (in secs) for web, ssh, telnet sessions: 3600
 Serial Console Session timeout(in secs): 600
 Serial Console Absolute Session timeout(in secs): 3600
 Admin Authentication server group:
 Operational Authentication server group:
 Use of 2nd factor: No
```

Set the Maximum Number of Login Attempts

You can configure the maximum number of failed login attempts allowed before a user is locked out of the Firepower 9300 chassis for a specified amount of time. If a user exceeds the set maximum number of login attempts, the user is locked out of the system. No notification appears indicating that the user is locked out. In this event, the user must wait the specified amount of time before attempting to log in.

Perform these steps to configure the maximum number of login attempts.

Note

-
- The default maximum number of unsuccessful login attempts is 3. The default amount of time the user is locked out of the system after exceeding the maximum number of login attemps is 60 minutes (3600 seconds).

Procedure

Step 1 From the FXOS CLI, enter security mode:

scope security

Step 2 Set the maximum number of unsuccessful login attempts.

set max-login-attempts *num_attempts*

Step 3 Specify the amount of time (in seconds) the user should remain locked out of the system after reaching the maximum number of login attempts:

set user-account-unlock-time

unlock_time

Step 4 Commit the configuration:

commit-buffer

Creating a Local User Account

Procedure

Step 1 Choose **System** > **User Management**.

Step 2 Click the **Local Users** tab.

Step 3 Click **Add User** to open the **Add User** dialog box.

Step 4 Complete the following fields with the required information about the user:

Name	Description
User Name field	The account name that is used when logging into this account. This name must be unique and meet the guidelines and restrictions for user account names (see Guidelines for Usernames, on page 22). After you save the user, the login ID cannot be changed. You must delete the user account and create a new one.
First Name field	The first name of the user. This field can contain up to 32 characters.
Last Name field	The last name of the user. This field can contain up to 32 characters.
Email field	The email address for the user.
Phone Number field	The telephone number for the user.

Name	Description
Password field	The password associated with this account. If password strength check is enabled, a user's password must be strong and the Firepower eXtensible Operating System rejects any password that does not meet the strength check requirements (see Guidelines for Passwords, on page 23). **Note** Passwords must not contain the following symbols: $ (dollar sign), ? (question mark), and = (equals sign). This restriction applies whether the password strength check is enabled or not.
Confirm Password field	The password a second time for confirmation purposes.
Account Status field	If the status is set to **Active**, a user can log into Firepower Chassis Manager and the FXOS CLI with this login ID and password.
User Role drop-down list	The role that represents the privileges you want to assign to the user account (see User Roles, on page 25). **Note** Changes in user roles and privileges do not take effect until the next time the user logs in. If a user is logged in when you assign a new role to or remove an existing role from a user account, the active session continues with the previous roles and privileges.
Account Expires check box	If checked, this account expires and cannot be used after the date specified in the **Expiration Date** field. **Note** After you configure a user account with an expiration date, you cannot reconfigure the account to not expire. You can, however, configure the account with the latest expiration date available.
Expiry Date field	The date on which the account expires. The date should be in the format yyyy-mm-dd. Click the calendar icon at the end of this field to view a calendar that you can use to select the expiration date.

Step 5 Click **Add**.

Deleting a Local User Account

Procedure

Step 1 Choose **System** > **User Management**.

Step 2 Click the **Local Users** tab.

Step 3 In the row for the user account that you want to delete, click **Delete**.

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

Activating or Deactivating a Local User Account

You must be a user with admin or AAA privileges to activate or deactivate a local user account.

Procedure

Step 1 Choose **System** > **User Management**.

Step 2 Click the **Local Users** tab.

Step 3 In the row for the user account that you want to activate or deactivate, click **Edit (pencil icon)**.

Step 4 In the **Edit User** dialog box, do one of the following:

- To activate a user account, click the **Active** radio button in the **Account Status** field. Note that when you reactivate a user account, the account password must be reset.
- To deactivate a user account, click the **Inactive** radio button in the **Account Status** field.

The admin user account is always set to active. It cannot be modified.

Step 5 Click **Save**.

Step 6 Commit the transaction to the system configuration:

Firepower-chassis /security/local-user # **commit-buffer**

Clearing the Password History for a Locally Authenticated User

Procedure

Step 1 Enter security mode:

Firepower-chassis # **scope security**

Step 2 Enter local user security mode for the specified user account:

Firepower-chassis /security # **scope local-user** *user-name*

Step 3 Clear the password history for the specified user account:

Firepower-chassis /security/local-user # **clear password-history**

Step 4 Commit the transaction to the system configuration:

Firepower-chassis /security/local-user # **commit-buffer**

Example

The following example clears the password history and commits the transaction:

```
Firepower-chassis # scope security
Firepower-chassis /security # scope local-user admin
Firepower-chassis /security/local-user # clear password-history
Firepower-chassis /security/local-user* # commit-buffer
Firepower-chassis /security/local-user #
```

CHAPTER 5

Image Management

About Image Management

The Firepower 9300 chassis uses two basic types of images:

Note All images are digitally signed and validated through Secure Boot. Do not modify the image in any way or you will receive a validation error.

- Platform Bundle—The Firepower platform bundle is a collection of multiple independent images that operate on the Firepower Supervisor and Firepower security module/engine. The platform bundle is a Firepower eXtensible Operating System software package.
- Application—Application images are the software images you want to deploy on the security module/engine of the Firepower 9300 chassis. Application images are delivered as Cisco Secure Package files (CSP) and are stored on the supervisor until deployed to a security module/engine as part of logical device creation or in preparation for later logical device creation. You can have multiple different versions of the same application image type stored on the Firepower Supervisor.

Note If you are upgrading both the Platform Bundle image and one or more Application images, you must upgrade the Platform Bundle first.

Downloading Images from Cisco.com

Download FXOS and application images from Cisco.com so you can upload them to the Firepower chassis.

Before you begin

You must have a Cisco.com account.

Procedure

Step 1 Using a web browser, navigate to http://www.cisco.com/go/firepower9300-software or http://www.cisco.com/go/firepower4100-software.
The software download page for the Firepower 9300 chassis is opened in the browser.

Step 2 Find and then download the appropriate software image to your local computer.

Uploading an Image to the Firepower Security Appliance

You can upload FXOS and application images to the chassis.

Before you begin

Make sure the image you want to upload is available on your local computer.

Procedure

Step 1 Choose **System** > **Updates**.
The Available Updates page shows a list of the Firepower eXtensible Operating System platform bundle images and application images that are available on the chassis.

Step 2 Click **Upload Image** to open the Upload Image dialog box.

Step 3 Click **Choose File** to navigate to and select the image that you want to upload.

Step 4 Click **Upload**.
The selected image is uploaded to the Firepower 9300 chassis.

Step 5 For certain software images you will be presented with an end-user license agreement after uploading the image. Follow the system prompts to accept the end-user license agreement.

Verifying the Integrity of an Image

The integrity of the image is automatically verified when a new image is added to the Firepower 9300 chassis. If needed, you can use the following procedure to manually verify the integrity of an image.

Procedure

Step 1 Choose **System** > **Updates**.
The Available Updates page shows a list of the Firepower eXtensible Operating System platform bundle images and application images that are available on the chassis.

Step 2 Click **Verify** (check mark icon) for the image you want to verify.

The system will verify the integrity of the image and display the staus in the Image Integrity field.

Upgrading the Firepower eXtensible Operating System Platform Bundle

Before you begin

Download the platform bundle software image from Cisco.com (see Downloading Images from Cisco.com, on page 36) and then upload that image to the Firepower 9300 chassis (see Uploading an Image to the Firepower Security Appliance, on page 36).

Procedure

Step 1 Choose **System** > **Updates**.
The Available Updates page shows a list of the Firepower eXtensible Operating System platform bundle images and application images that are available on the chassis.

Step 2 Click **Upgrade** for the FXOS platform bundle to which you want to upgrade.

The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

Step 3 Click **Yes** to confirm that you want to proceed with installation, or click **No** to cancel the installation.

The Firepower eXtensible Operating System unpacks the bundle and upgrades/reloads the components.

Downloading a Logical Device Software Image to the Firepower 9300 chassis

You can use FTP, SCP, SFTP, or TFTP to copy the logical device software image to the Firepower 9300 chassis.

Before you begin

Collect the following information that you will need to import a configuration file:

- IP address and authentication credentials for the server from which you are copying the image
- Fully qualified name of the software image file

Procedure

Step 1 Enter Security Services mode:

Firepower-chassis # **scope ssa**

Step 2 Enter Application Software mode:

Firepower-chassis /ssa # **scope app-software**

Step 3 Download the logical device software image:

Firepower-chassis /ssa/app-software # **download image** *URL*

Specify the URL for the file being imported using one of the following syntax:

- **ftp**://*username*@*hostname*/*path*
- **scp**://*username*@*hostname*/*path*
- **sftp**://*username*@*hostname*/*path*
- **tftp**://*hostname*:*port-num*/*path*

Step 4 To monitor the download process:

Firepower-chassis /ssa/app-software # **show download-task**

Step 5 To view the downloaded applications:

Firepower-chassis /ssa/app-software # **up**

Firepower-chassis /ssa # **show app**

Step 6 To view details for a specific application:

Firepower-chassis /ssa # **scope app** *application_type image_version*

Firepower-chassis /ssa/app # **show expand**

Example

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
```

```
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                      Protocol   Server               Userid          State
    ------------------------------ ---------- -------------------- --------------- -----
   cisco-asa.9.4.1.65.csp        Scp       192.168.1.1         user           Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes

Firepower-chassis /ssa # scope app asa 9.4.1.65
Firepower-chassis /ssa/app # show expand

Application:
    Name: asa
    Version: 9.4.1.65
    Description: N/A
    Author:
    Deploy Type: Native
    CSP Type: Application
    Is Default App: Yes

    App Attribute Key for the Application:
        App Attribute Key Description
        ----------------- -----------
        cluster-role      This is the role of the blade in the cluster
        mgmt-ip           This is the IP for the management interface
        mgmt-url          This is the management URL for this application

    Net Mgmt Bootstrap Key for the Application:
        Bootstrap Key Key Data Type Is the Key Secret Description
        ------------- ------------- ----------------- -----------
        PASSWORD      String        Yes               The admin user password.

    Port Requirement for the Application:
        Port Type: Data
        Max Ports: 120
        Min Ports: 1

        Port Type: Mgmt
        Max Ports: 1
        Min Ports: 1

        Mgmt Port Sub Type for the Application:
            Management Sub Type
            -------------------
            Default

        Port Type: Cluster
        Max Ports: 1
        Min Ports: 0
Firepower-chassis /ssa/app #
```

Updating the Image Version for a Logical Device

Use this procedure to upgrade the ASA application image to a new version, or set the Firepower Threat Defense application image to a new startup version that will be used in a disaster recovery scenario.

When you change the startup version on an ASA logical device, the ASA upgrades to that version and all configuration is restored. Use the following workflows to change the ASA startup version, depending on your configuration:

ASA High Availability -

1. Change the logical device image version(s) on the standby unit.
2. Make the standby unit active.
3. Change the application version(s) on the other unit.

ASA Inter-Chassis Cluster -

1. Change the startup version on the data unit.
2. Make the data unit the control unit.
3. Change the startup version on the original control unit (now data).

Before you begin

Download the application image you want to use for the logical device from Cisco.com (see Downloading Images from Cisco.com, on page 36) and then upload that image to the Firepower 9300 chassis (see Uploading an Image to the Firepower Security Appliance, on page 36).

If you are upgrading both the Platform Bundle image and one or more Application images, you must upgrade the Platform Bundle first.

Procedure

Step 1 Choose **Logical Devices** to open the Logical Devices page.
The Logical Devices page shows a list of configured logical devices on the chassis. If no logical devices have been configured, a message stating so is shown instead.

Step 2 Click **Update Version** for the logical device that you want to update to open the **Update Image Version** dialog box.

Step 3 For the **New Version**, choose the software version.

Step 4 Click **OK**.

Firmware Upgrade

For information about upgrading the firmware on your Firepower 9300 chassis, see the *Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide*.

CHAPTER 6

Platform Settings

Changing the Management IP Address

Before you begin

You can change the management IP address on the Firepower 9300 chassis from the FXOS CLI.

Note After changing the management IP address, you will need to reestablish any connections to Firepower Chassis Manager or the FXOS CLI using the new address.

Procedure

Step 1 Connect to the FXOS CLI (see Accessing the FXOS CLI, on page 8).

Step 2 To configure an IPv4 management IP address:

a) Set the scope for fabric-interconnect a:

   Firepower-chassis# **scope fabric-interconnect a**

b) To view the current management IP address, enter the following command:

   Firepower-chassis /fabric-interconnect # **show**

c) Enter the following command to configure a new management IP address and gateway:

Firepower-chassis /fabric-interconnect # **set out-of-band ip** *ip_address* **netmask** *network_mask* **gw** *gateway_ip_address*

d) Commit the transaction to the system configuration:

Firepower-chassis /fabric-interconnect* # **commit-buffer**

Step 3 To configure an IPv6 management IP address:

a) Set the scope for fabric-interconnect a:

Firepower-chassis# **scope fabric-interconnect a**

b) Set the scope for management IPv6 configuration:

Firepower-chassis /fabric-interconnect # **scope ipv6-config**

c) To view the current management IPv6 address, enter the following command:

Firepower-chassis /fabric-interconnect/ipv6-config # **show ipv6-if**

d) Enter the following command to configure a new management IP address and gateway:

Firepower-chassis /fabric-interconnect/ipv6-config # **set out-of-band ipv6** *ipv6_address* **ipv6-prefix** *prefix_length* **ipv6-gw** *gateway_address*

Note Only IPv6 Global Unicast addresses are supported as the chassis's IPv6 management address.

e) Commit the transaction to the system configuration:

Firepower-chassis /fabric-interconnect/ipv6-config* # **commit-buffer**

Example

The following example configures an IPv4 management interface and gateway:

```
Firepower-chassis# scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # show

Fabric Interconnect:
    ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6 Gateway
 Prefix Operability
    ---- --------------- --------------- --------------- ---------------- ----------------
 ------ -----------
    A    192.0.2.112     192.0.2.1       255.255.255.0   ::               ::
 64     Operable
Firepower-chassis /fabric-interconnect # set out-of-band ip 192.0.2.111 netmask 255.255.255.0
 gw 192.0.2.1
Warning: When committed, this change may disconnect the current CLI session
Firepower-chassis /fabric-interconnect* #commit-buffer
Firepower-chassis /fabric-interconnect #
```

The following example configures an IPv6 management interface and gateway:

```
Firepower-chassis# scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # scope ipv6-config
```

```
Firepower-chassis /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
    IPv6 Address                        Prefix     IPv6 Gateway
    ----------------------------------- ---------- ------------
    2001::8998                          64         2001::1
Firepower-chassis /fabric-interconnect/ipv6-config # set out-of-band ipv6 2001::8999
ipv6-prefix 64 ipv6-gw 2001::1
Firepower-chassis /fabric-interconnect/ipv6-config* # commit-buffer
Firepower-chassis /fabric-interconnect/ipv6-config #
```

Setting the Date and Time

Use the NTP page to configure the network time protocol (NTP) on the system, to set the date and time manually, or to view the current system time.

NTP settings are automatically synced between the Firepower 9300 chassis and any logical devices installed on the chassis.

Setting the Time Zone

Procedure

Step 1 Choose **Platform Settings** > **NTP**.

Step 2 Choose the appropriate time zone for the Firepower chassis from the **Time Zone** drop-down list.

Setting the Date and Time Using NTP

NTP is used to implement a hierarchical system of servers that provide a precisely synchronized time among network systems. This kind of accuracy is required for time-sensitive operations, such as validating CRLs, which include a precise time stamp.

Before you begin

If you use a hostname for the NTP server, you must configure a DNS server. See Configuring DNS Servers, on page 78.

Procedure

Step 1 Choose **Platform Settings** > **NTP**.

Step 2 Under **Set Time Source**, click **Use NTP Server** and then enter the IP address or hostname of the NTP server you want to use in the **NTP Server** field.

Step 3 Click **Save**.

Note If you modify the system time by more than 10 minutes, the system will log you out and you will need to log in to the Firepower Chassis Manager again.

Deleting an NTP Server

Procedure

Step 1 Choose **Platform Settings** > **NTP**.

Step 2 To stop using the NTP server, configure the system to use a manually configured date and time (see Setting the Date and Time Manually, on page 44).

Step 3 Click **Save**.

Setting the Date and Time Manually

This section describes how to set the date and time manually on the Firepower chassis.

Procedure

Step 1 Choose **Platform Settings** > **NTP**.

Step 2 Under **Set Time Source**, click **Set Time Manually**.

Step 3 Click the **Date** drop-down list to display a calendar and then set the date using the controls available in the calendar.

Step 4 Use the corresponding drop-down lists to specify the time as hours, minutes, and AM/PM.

Tip You can click **Get System Time** to set the date and time to match what is configured on the system you are using to connect to the Firepower Chassis Manager.

Step 5 Click **Save**.

The Firepower chassis is configured with the date and time specified.

Note If you modify the system time by more than 10 minutes, the system will log you out and you will need to log in to the Firepower Chassis Manager again.

Configuring SSH

The following procedure describes how to enable or disable SSH access to the Firepower chassis, how to enable the FXOS chassis as an SSH client, and how to configure the various algorithms used by SSH for encryption, key exchange, and message authentication for both the SSH server and SSH client.

SSH is enabled by default.

Procedure

Step 1 Choose **Platform Settings** > **SSH** > **SSH Server**.

Step 2 To enable SSH access to the Firepower chassis, check the **Enable SSH** check box. To disable SSH access, uncheck the **Enable SSH** check box.

Step 3 Click **Save**.

Configuring Telnet

The following procedure describes how to enable or disable Telnet access to the Firepower chassis. Telnet is disabled by default.

Note Telnet configuration is currently only available using the CLI.

Procedure

Step 1 Enter system mode:

Firepower-chassis # **scope system**

Step 2 Enter system services mode:

Firepower-chassis /system # **scope services**

Step 3 To configure Telnet access to the Firepower chassis, do one of the following:

- To allow Telnet access to the Firepower chassis, enter the following command:

  Firepower-chassis /system/services # **enable telnet-server**

- To disallow Telnet access to the Firepower chassis, enter the following command:

  Firepower-chassis /system/services # **disable telnet-server**

Step 4 Commit the transaction to the system configuration:

Firepower /system/services # **commit-buffer**

Example

The following example enables Telnet and commits the transaction:

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /services # enable telnet-server
Firepower-chassis /services* # commit-buffer
Firepower-chassis /services #
```

Configuring SNMP

Use the SNMP page to configure the Simple Network Management Protocol (SNMP) on the Firepower chassis. See the following topics for more information:

About SNMP

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network.

The SNMP framework consists of three parts:

- An SNMP manager—The system used to control and monitor the activities of network devices using SNMP.
- An SNMP agent—The software component within the Firepower chassis that maintains the data for the Firepower chassis and reports the data, as needed, to the SNMP manager. The Firepower chassis includes the agent and a collection of MIBs. To enable the SNMP agent and create the relationship between the manager and agent, enable and configure SNMP in the Firepower Chassis Manager or the FXOS CLI.
- A managed information base (MIB)—The collection of managed objects on the SNMP agent.

The Firepower chassis supports SNMPv1, SNMPv2c and SNMPv3. Both SNMPv1 and SNMPv2c use a community-based form of security. SNMP is defined in the following:

- RFC 3410 (http://tools.ietf.org/html/rfc3410)
- RFC 3411 (http://tools.ietf.org/html/rfc3411)
- RFC 3412 (http://tools.ietf.org/html/rfc3412)
- RFC 3413 (http://tools.ietf.org/html/rfc3413)
- RFC 3414 (http://tools.ietf.org/html/rfc3414)
- RFC 3415 (http://tools.ietf.org/html/rfc3415)
- RFC 3416 (http://tools.ietf.org/html/rfc3416)
- RFC 3417 (http://tools.ietf.org/html/rfc3417)
- RFC 3418 (http://tools.ietf.org/html/rfc3418)
- RFC 3584 (http://tools.ietf.org/html/rfc3584)

Note Be aware that SNMP versions 1 and 2c have serious known security issues: they transmit all information without encryption, including the community string, which serves as the only form of authentication in these versions.

SNMP Notifications

A key feature of SNMP is the ability to generate notifications from an SNMP agent. These notifications do not require that requests be sent from the SNMP manager. Notifications can indicate improper user authentication, restarts, the closing of a connection, loss of connection to a neighbor router, or other significant events.

The Firepower chassis generates SNMP notifications as either traps or informs. Traps are less reliable than informs because the SNMP manager does not send any acknowledgment when it receives a trap, and the Firepower chassis cannot determine if the trap was received. An SNMP manager that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the Firepower chassis does not receive the PDU, it can send the inform request again.

However, informs are available only with SNMPv2c, which is considered insecure, and is not recommended.

SNMP Security Levels and Privileges

SNMPv1, SNMPv2c, and SNMPv3 each represent a different security model. The security model combines with the selected security level to determine the security mechanism applied when the SNMP message is processed.

The security level determines the privileges required to view the message associated with an SNMP trap. The privilege level determines whether the message needs to be protected from disclosure or authenticated. The supported security level depends upon which security model is implemented. SNMP security levels support one or more of the following privileges:

- noAuthNoPriv—No authentication or encryption
- authNoPriv—Authentication but no encryption
- authPriv—Authentication and encryption

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

Supported Combinations of SNMP Security Models and Levels

The following table identifies what the combinations of security models and levels mean.

Table 1: SNMP Security Models and Levels

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication. **Note** While you can configure it, FXOS does not support use of `noAuthNoPriv` with SNMP version 3.
v3	authNoPriv	HMAC-SHA	No	Provides authentication based on the HMAC Secure Hash Algorithm (SHA).
v3	authPriv	HMAC-SHA	DES	Provides authentication based on the HMAC-SHA algorithm. Provides Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.

SNMPv3 Security Features

SNMPv3 provides secure access to devices by a combination of authenticating and encrypting frames over the network. SNMPv3 authorizes management operations only by configured users and encrypts SNMP messages. The SNMPv3 User-Based Security Model (USM) refers to SNMP message-level security and offers the following services:

- Message integrity—Ensures that messages have not been altered or destroyed in an unauthorized manner and that data sequences have not been altered to an extent greater than can occur non-maliciously.
- Message origin authentication—Ensures that the claimed identity of the user on whose behalf received data was originated is confirmed.
- Message confidentiality and encryption—Ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.

SNMP Support

The Firepower chassis provides the following support for SNMP:

Support for MIBs

The Firepower chassis supports read-only access to MIBs.

For information about the specific MIBs available and where you can obtain them, see the Cisco FXOS MIB Reference Guide.

Authentication Protocol for SNMPv3 Users

The Firepower chassis supports the HMAC-SHA-96 (SHA) authentication protocol for SNMPv3 users.

AES Privacy Protocol for SNMPv3 Users

The Firepower chassis uses Advanced Encryption Standard (AES) as one of the privacy protocols for SNMPv3 message encryption and conforms with RFC 3826.

The privacy password, or priv option, offers a choice of DES or 128-bit AES encryption for SNMP security encryption. If you enable AES-128 configuration and include a privacy password for an SNMPv3 user, the Firepower chassis uses the privacy password to generate a 128-bit AES key. The AES privacy password can have a minimum of eight characters. If the passphrases are specified in clear text, you can specify a maximum of 64 characters.

Enabling SNMP and Configuring SNMP Properties

Procedure

Step 1 Choose **Platform Settings** > **SNMP**.

Step 2 In the **SNMP** area, complete the following fields:

Name	Description
Admin State check box	Whether SNMP is enabled or disabled. Enable this service only if your system includes integration with an SNMP server.
Port field	The port on which the Firepower chassis communicates with the SNMP host. You cannot change the default port.

Name	Description
Community/Username field	(Optional) The community string used for polling in SNMP v1 and v2. When you specify an SNMP community name, you are also automatically enabling SNMP versions 1 and 2c for polling requests from the SNMP remote manager. This field is not applicable to SNMP v3. Be aware that SNMP versions 1 and 2c have serious known security issues: they transmit all information without encryption, including the community string, which serves as the only form of authentication in these versions. Enter an alphanumeric string between 1 and 32 characters. Do not use @ (at sign), \ (backslash), " (double quote), ? (question mark) or an empty space. The default is `public`. If the **Community/Username** field is already set, the text to the right of the empty field reads **Set: Yes**. If the **Community/Username** field is not yet populated with a value, the text to the right of the empty field reads **Set: No**. **Note** You can use the CLI command **set snmp community** to delete an existing community string, thereby disabling SNMP versions 1 and 2c for polling requests from the SNMP remote manager.
System Administrator Name field	The contact person responsible for the SNMP implementation. Enter a string of up to 255 characters, such as an email address or a name and telephone number.
Location field	The location of the host on which the SNMP agent (server) runs. Enter an alphanumeric string up to 510 characters.

Step 3 Click **Save**.

What to do next

Create SNMP traps and users.

Creating an SNMP Trap

The following procedure describes how to create SNMP traps.

Note You can define up to eight SNMP traps.

Procedure

Step 1 Choose **Platform Settings** > **SNMP**.

Step 2 In the **SNMP Traps** area, click **Add**.

Step 3 In the **Add SNMP Trap** dialog box, complete the following fields:

Name	Description
Host Name field	The hostname or IP address of the SNMP host to which the Firepower chassis should send the traps.
Community/Username field	Enter the SNMPv1/v2c community string, or the SNMPv3 user name, needed to permit access to the trap destination. This must be the same as the community or user name that is configured for the SNMP service. Enter an alphanumeric string between 1 and 32 characters. Do not use @ (at sign), \ (backslash), " (double quote), ? (question mark) or an empty space.
Port field	The port on which the Firepower chassis communicates with the SNMP host for the trap. Enter an integer between 1 and 65535.
Version field	The SNMP version and model used for the trap. This can be one of the following: • **V1** • **V2** • **V3** **Note** Be aware that SNMP versions 1 and 2c have serious known security issues: they transmit all information without encryption, including the community string, which serves as the only form of authentication in these versions.
Type field	Specify the type of trap to send: • **Traps** • **Informs** (only valid when **Version** is **V2**)
v3 Privilege field	If you selected **V3** for the version, specify the privilege level associated with the trap: • **Auth**—Authentication but no encryption. • **Noauth**—No authentication or encryption. Note that while you can select it, FXOS does not support this security level with SNMPv3. • **Priv**—Authentication and encryption.

Step 4 Click **OK** to close the **Add SNMP Trap** dialog box.

Step 5 Click **Save**.

Deleting an SNMP Trap

Procedure

Step 1 Choose **Platform Settings** > **SNMP**.

Step 2 In the **SNMP Traps** area, click the **Delete** icon in the row in the table that corresponds to the trap you want to delete.

Creating an SNMPv3 User

Procedure

Step 1 Choose **Platform Settings** > **SNMP**.

Step 2 In the **SNMP Users** area, click **Add**.

Step 3 In the **Add SNMP User** dialog box, complete the following fields:

Name	Description
Name field	The user name assigned to the SNMPv3 user. Enter up to 32 characters. The name must begin with a letter. Valid characters include letters, numbers, _ (underscore), . (period), @ (at sign), and - (hyphen).
Auth Type field	The authorization type: **SHA**.
Use AES-128 check box	If checked, this user uses AES-128 encryption.

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Password field</td><td>The password for this user.

The Firepower eXtensible Operating System rejects any password that does not meet the following requirements:

• Must contain a minimum of 8 characters and a maximum of 80 characters.

• Must contain only letters, numbers, and the following characters:

~`!@#%^&*()_-+{}[]|\:;"'<,>./

• Must not contain the following symbols: $ (dollar sign), ? (question mark), or = (equals sign).

• Must contain at least five different characters.

• Must not contain too many consecutively incrementing or decrementing numbers or letters. For example, the string "12345" has four such characters, and the string "ZYXW" has three. If the total number of such characters exceeds a certain limit (typically more than around 4-6 such occurrences), the simplicity check will fail.

Note The consecutively incrementing or decrementing character count is not reset when non-incrementing or decrementing characters are used in between. For example, abcd&!21 will fail the password check, but abcd&!25, will not.</td></tr>
<tr><td>Confirm Password field</td><td>The password again for confirmation purposes.</td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Privacy Password field</td><td>The privacy password for this user.

The Firepower eXtensible Operating System rejects any password that does not meet the following requirements:

• Must contain a minimum of 8 characters and a maximum of 80 characters.

• Must contain only letters, numbers, and the following characters:

~`!@#%^&*()_-+{}[]|\:;"'<,>./

• Must not contain the following symbols: $ (dollar sign), ? (question mark), or = (equals sign).

• Must contain at least five different characters.

• Must not contain too many consecutively incrementing or decrementing numbers or letters. For example, the string "12345" has four such characters, and the string "ZYXW" has three. If the total number of such characters exceeds a certain limit (typically more than around 4-6 such occurrences), the simplicity check will fail.

Note The consecutively incrementing or decrementing character count is not reset when non-incrementing or decrementing characters are used in between. For example, abcd&!21 will fail the password check, but abcd&!25, will not.</td></tr>
<tr><td>Confirm Privacy Password field</td><td>The privacy password again for confirmation purposes.</td></tr>
</table>

Step 4 Click **OK** to close the **Add SNMP User** dialog box.

Step 5 Click **Save**.

Deleting an SNMPv3 User

Procedure

Step 1 Choose **Platform Settings** > **SNMP**.

Step 2 In the **SNMP Users** area, click the **Delete** icon in the row in the table that corresponds to the user you want to delete.

Configuring HTTPS

This section describes how to configure HTTPS on the Firepower 9300 chassis.

Note You can change the HTTPS port using Firepower Chassis Manager or the FXOS CLI. All other HTTPS configuration can only be done using the FXOS CLI.

Certificates, Key Rings, and Trusted Points

HTTPS uses components of the Public Key Infrastructure (PKI) to establish secure communications between two devices, such as a client's browser and the Firepower 9300 chassis.

Encryption Keys and Key Rings

Each PKI device holds a pair of asymmetric Rivest-Shamir-Adleman (RSA) encryption keys, one kept private and one made public, stored in an internal key ring. A message encrypted with either key can be decrypted with the other key. To send an encrypted message, the sender encrypts the message with the receiver's public key, and the receiver decrypts the message using its own private key. A sender can also prove its ownership of a public key by encrypting (also called 'signing') a known message with its own private key. If a receiver can successfully decrypt the message using the public key in question, the sender's possession of the corresponding private key is proven. Encryption keys can vary in length, with typical lengths from 512 bits to 2048 bits. In general, a longer key is more secure than a shorter key. FXOS provides a default key ring with an initial 2048-bit key pair, and allows you to create additional key rings.

The default key ring certificate must be manually regenerated if the cluster name changes or the certificate expires.

Certificates

To prepare for secure communications, two devices first exchange their digital certificates. A certificate is a file containing a device's public key along with signed information about the device's identity. To merely support encrypted communications, a device can generate its own key pair and its own self-signed certificate. When a remote user connects to a device that presents a self-signed certificate, the user has no easy method to verify the identity of the device, and the user's browser will initially display an authentication warning. By default, FXOS contains a built-in self-signed certificate containing the public key from the default key ring.

Trusted Points

To provide stronger authentication for FXOS, you can obtain and install a third-party certificate from a trusted source, or trusted point, that affirms the identity of your device. The third-party certificate is signed by the issuing trusted point, which can be a root certificate authority (CA) or an intermediate CA or trust anchor that is part of a trust chain that leads to a root CA. To obtain a new certificate, you must generate a certificate request through FXOS and submit the request to a trusted point.

Important The certificate must be in Base64 encoded X.509 (CER) format.

Creating a Key Ring

FXOS supports a maximum of 8 key rings, including the default key ring.

Procedure

Step 1 Enter security mode:

Firepower-chassis # **scope security**

Step 2 Create and name the key ring:

Firepower-chassis # **create keyring** *keyring-name*

Step 3 Set the SSL key length in bits:

Firepower-chassis # **set modulus** {**mod1024** | **mod1536** | **mod2048** | **mod512**}

Step 4 Commit the transaction:

Firepower-chassis # **commit-buffer**

Example

The following example creates a keyring with a key size of 1024 bits:

```
Firepower-chassis# scope security
Firepower-chassis /security # create keyring kr220
Firepower-chassis /security/keyring* # set modulus mod1024
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring #
```

What to do next

Create a certificate request for this key ring.

Regenerating the Default Key Ring

The default key ring certificate must be manually regenerated if the cluster name changes or the certificate expires.

Procedure

Step 1 Enter security mode:

Firepower-chassis # **scope security**

Step 2 Enter key ring security mode for the default key ring:

Firepower-chassis /security # **scope keyring default**

Step 3 Regenerate the default key ring:

Firepower-chassis /security/keyring # **set regenerate yes**

Step 4 Commit the transaction:

Firepower-chassis # **commit-buffer**

Example

The following example regenerates the default key ring:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring default
Firepower-chassis /security/keyring* # set regenerate yes
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring #
```

Creating a Certificate Request for a Key Ring

Creating a Certificate Request for a Key Ring with Basic Options

Procedure

Step 1 Enter security mode:

Firepower-chassis # **scope security**

Step 2 Enter configuration mode for the key ring:

Firepower-chassis /security # **scope keyring** *keyring-name*

Step 3 Create a certificate request using the IPv4 or IPv6 address specified, or the name of the fabric interconnect. You are prompted to enter a password for the certificate request.

Firepower-chassis /security/keyring # **create certreq** {**ip** [*ipv4-addr* | *ipv6-v6*] |**subject-name** *name*}

Step 4 Commit the transaction:

Firepower-chassis /security/keyring/certreq # **commit-buffer**

Step 5 Display the certificate request, which you can copy and send to a trust anchor or certificate authority:

Firepower-chassis /security/keyring # **show certreq**

Example

The following example creates and displays a certificate request with an IPv4 address for a key ring, with basic options:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # create certreq ip 192.168.200.123 subject-name sjc04
Certificate request password:
Confirm certificate request password:
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request e-mail name:
Certificate request country name:
State, province or county (full name):
Locality (eg, city):
Organization name (eg, company):
Organization Unit name (eg, section):
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF8OPhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1WsylwUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHUO03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWIcTWgHhH8BimOb/0OKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGxlDNqoN+odCXPc5kjoXD0lZTL09H
BA==
-----END CERTIFICATE REQUEST-----

Firepower-chassis /security/keyring #
```

What to do next

- Copy the text of the certificate request, including the BEGIN and END lines, and save it in a file. Send the file with the certificate request to a trust anchor or certificate authority to obtain a certificate for the key ring.
- Create a trusted point and set the certificate chain for the certificate of trust received from the trust anchor.

Creating a Certificate Request for a Key Ring with Advanced Options

Procedure

Step 1 Enter security mode:

Firepower-chassis # **scope security**

Step 2 Enter configuration mode for the key ring:

Firepower-chassis /security # **scope keyring** *keyring-name*

Step 3 Create a certificate request:

Firepower-chassis /security/keyring # **create certreq**

Step 4 Specify the country code of the country in which the company resides:

Firepower-chassis /security/keyring/certreq* # **set country** *country name*

Step 5 Specify the Domain Name Server (DNS) address associated with the request:

Firepower-chassis /security/keyring/certreq* # **set dns** *DNS Name*

Step 6 Specify the email address associated with the certificate request:

Firepower-chassis /security/keyring/certreq* # **set e-mail** *E-mail name*

Step 7 Specify the IP address of the Firepower 9300 chassis:

Firepower-chassis /security/keyring/certreq* # **set ip** {*certificate request ip-address*|*certificate request ip6-address* }

Step 8 Specify the city or town in which the company requesting the certificate is headquartered:

Firepower-chassis /security/keyring/certreq* # **set locality** *locality name (eg, city)*

Step 9 Specify the organization requesting the certificate:

Firepower-chassis /security/keyring/certreq* # **set org-name** *organization name*

Step 10 Specify the organizational unit:

Firepower-chassis /security/keyring/certreq* # **set org-unit-name** *organizational unit name*

Step 11 Specify an optional password for the certificate request:

Firepower-chassis /security/keyring/certreq* # **set password** *certificate request password*

Step 12 Specify the state or province in which the company requesting the certificate is headquartered:

Firepower-chassis /security/keyring/certreq* # **set state** *state, province or county*

Step 13 Specify the fully qualified domain name of the Firepower 9300 chassis:

Firepower-chassis /security/keyring/certreq* # **set subject-name** *certificate request name*

Step 14 Commit the transaction:

Firepower-chassis /security/keyring/certreq # **commit-buffer**

Step 15 Display the certificate request, which you can copy and send to a trust anchor or certificate authority:

Firepower-chassis /security/keyring # **show certreq**

Example

The following example creates and displays a certificate request with an IPv4 address for a key ring, with advanced options:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # create certreq
Firepower-chassis /security/keyring/certreq* # set ip 192.168.200.123
Firepower-chassis /security/keyring/certreq* #  set subject-name sjc04
Firepower-chassis /security/keyring/certreq* # set country US
Firepower-chassis /security/keyring/certreq* # set dns bg1-samc-15A
Firepower-chassis /security/keyring/certreq* # set email test@cisco.com
Firepower-chassis /security/keyring/certreq* # set locality new york city
```

```
Firepower-chassis /security/keyring/certreq* # set org-name "Cisco Systems"
Firepower-chassis /security/keyring/certreq* # set org-unit-name Testing
Firepower-chassis /security/keyring/certreq* # set state new york
Firepower-chassis /security/keyring/certreq* # commit-buffer
Firepower-chassis /security/keyring/certreq # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request e-mail name: test@cisco.com
Certificate request country name: US
State, province or county (full name): New York
Locality name (eg, city): new york city
Organization name (eg, company): Cisco
Organization Unit name (eg, section): Testing
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF8OPhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1WsylwUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHUO03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWIcTWgHhH8BimOb/0OKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGxlDNqoN+odCXPc5kjoXD0lZTL09H
BA==
-----END CERTIFICATE REQUEST-----

Firepower-chassis /security/keyring/certreq #
```

What to do next

- Copy the text of the certificate request, including the BEGIN and END lines, and save it in a file. Send the file with the certificate request to a trust anchor or certificate authority to obtain a certificate for the key ring.
- Create a trusted point and set the certificate chain for the certificate of trust received from the trust anchor.

Creating a Trusted Point

Procedure

Step 1 Enter security mode:

Firepower-chassis # **scope security**

Step 2 Create a trusted point:

Firepower-chassis /security # **create trustpoint** *name*

Step 3 Specify certificate information for this trusted point:

Firepower-chassis /security/trustpoint # **set certchain** [*certchain*]

If you do not specify certificate information in the command, you are prompted to enter a certificate or a list of trustpoints defining a certification path to the root certificate authority (CA). On the next line following your input, type **ENDOFBUF** to finish.

Important The certificate must be in Base64 encoded X.509 (CER) format.

Step 4 Commit the transaction:

Firepower-chassis /security/trustpoint # **commit-buffer**

Example

The following example creates a trusted point and provides a certificate for the trusted point:

```
Firepower-chassis# scope security
Firepower-chassis /security # create trustpoint tPoint10
Firepower-chassis /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
> -----BEGIN CERTIFICATE-----
> MIIDMDCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJVUzEL
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> jtcEMyZ+f7+3yh421ido3nO4MIGeBgNVHSMEgZYwgZOAFLlNjtcEMyZ+f7+3yh42
> 1ido3nO4oXikdjB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFDASBgNVBAcT
> C1NhbnRhIENsYXJhMRswGQYDVQQKExJOdW92YSBTeXN0ZW1zIEluYy4xFDASBgNV
> BAsTC0VuZ2luZWVyaW5nMQ8wDQYDVQQDEwZ0ZXN0Q0GCAQAwDAYDVR0TBAUwAwEB
> /zANBgkqhkiG9w0BAQQFAAOBgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQqXc
> wR4pYiO4z42/j9Ijenh75tCKMhW51az8copP1EBmOcyuhf5C6vasrenn1ddkkYt4
> PR0vxGc40whuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6id1avt
> 4YL5Jg==
> -----END CERTIFICATE-----
> ENDOFBUF
Firepower-chassis /security/trustpoint* # commit-buffer
Firepower-chassis /security/trustpoint #
```

What to do next

Obtain a key ring certificate from the trust anchor or certificate authority and import it into the key ring.

Importing a Certificate into a Key Ring

Before you begin

- Configure a trusted point that contains the certificate chain for the key ring certificate.
- Obtain a key ring certificate from a trust anchor or certificate authority.

Procedure

Step 1 Enter security mode:

Firepower-chassis # **scope security**

Step 2 Enter configuration mode for the key ring that will receive the certificate:

Firepower-chassis /security # **scope keyring** *keyring-name*

Step 3 Specify the trusted point for the trust anchor or certificate authority from which the key ring certificate was obtained:

Firepower-chassis /security/keyring # **set trustpoint** *name*

Step 4 Launch a dialog for entering and uploading the key ring certificate:

Firepower-chassis /security/keyring # **set cert**

At the prompt, paste the certificate text that you received from the trust anchor or certificate authority. On the next line following the certificate, type **`ENDOFBUF`** to complete the certificate input.

Important The certificate must be in Base64 encoded X.509 (CER) format.

Step 5 Commit the transaction:

Firepower-chassis /security/keyring # **commit-buffer**

Example

The following example specifies the trust point and imports a certificate into a key ring:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # set trustpoint tPoint10
Firepower-chassis /security/keyring* # set cert
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
> -----BEGIN CERTIFICATE-----
> MIIB/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
> -----END CERTIFICATE-----
> ENDOFBUF
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring #
```

What to do next

Configure your HTTPS service with the key ring.

Configuring HTTPS

Caution After you complete the HTTPS configuration, including changing the port and key ring to be used by HTTPS, all current HTTP and HTTPS sessions are closed without warning as soon as you save or commit the transaction.

Procedure

Step 1 Enter system mode:

Firepower-chassis# **scope system**

Step 2 Enter system services mode:

Firepower-chassis /system # **scope services**

Step 3 Enable the HTTPS service:

Firepower-chassis /system/services # **enable https**

Step 4 (Optional) Specify the port to be used for the HTTPS connection:

Firepower-chassis /system/services # **set https port** *port-num*

Step 5 (Optional) Specify the name of the key ring you created for HTTPS:

Firepower-chassis /system/services # **set https keyring** *keyring-name*

Step 6 (Optional) Specify the level of Cipher Suite security used by the domain:

Firepower-chassis /system/services # **set https cipher-suite-mode** *cipher-suite-mode*

cipher-suite-mode can be one of the following keywords:

- **high-strength**
- **medium-strength**
- **low-strength**
- **custom**—Allows you to specify a user-defined Cipher Suite specification string.

Step 7 (Optional) If **cipher-suite-mode** is set to **custom**, specify a custom level of Cipher Suite security for the domain:

Firepower-chassis /system/services # **set https cipher-suite** *cipher-suite-spec-string*

cipher-suite-spec-string can contain up to 256 characters and must conform to the OpenSSL Cipher Suite specifications. You cannot use any spaces or special characters except ! (exclamation point), + (plus sign), - (hyphen), and : (colon). For details, see http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite.

For example, the medium strength specification string FXOS uses as the default is:
`ALL:!ADH:!EXPORT56:!LOW:RC4+RSA:+HIGH:+MEDIUM:+EXP:+eNULL`

Note This option is ignored if **cipher-suite-mode** is set to anything other than **custom**.

Step 8 Commit the transaction to the system configuration:

Firepower-chassis /system/services # **commit-buffer**

Example

The following example enables HTTPS, sets the port number to 443, sets the key ring name to kring7984, sets the Cipher Suite security level to high, and commits the transaction:

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # enable https
Firepower-chassis /system/services* # set https port 443
Warning: When committed, this closes all the web sessions.
Firepower-chassis /system/services* # set https keyring kring7984
Firepower-chassis /system/services* # set https cipher-suite-mode high
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

Changing the HTTPS Port

The HTTPS service is enabled on port 443 by default. You cannot disable HTTPS, but you can change the port to use for HTTPS connections.

Procedure

Step 1 Choose **Platform Settings** > **HTTPS**.

Step 2 Enter the port to use for HTTPS connections in the **Port** field. Specify an integer between 1 and 65535. This service is enabled on port 443 by default.

Step 3 Click **Save**.

The Firepower chassis is configured with the HTTPS port specified.

After changing the HTTPS port, all current HTTPS sessions are closed. Users will need to log back in to the Firepower Chassis Manager using the new port as follows:

`https://<chassis_mgmt_ip_address>:<chassis_mgmt_port>`

where <*chassis_mgmt_ip_address*> is the IP address or host name of the Firepower chassis that you entered during initial configuration and <*chassis_mgmt_port*> is the HTTPS port you have just configured.

Deleting a Key Ring

Procedure

Step 1 Enter security mode:

Firepower-chassis # **scope security**

Step 2 Delete the named key ring:

Firepower-chassis /security # **delete keyring** *name*

Step 3 Commits the transaction:

Firepower-chassis /security # **commit-buffer**

Example

The following example deletes a key ring:

```
Firepower-chassis# scope security
Firepower-chassis /security # delete keyring key10
Firepower-chassis /security* # commit-buffer
Firepower-chassis /security #
```

Deleting a Trusted Point

Before you begin

Ensure that the trusted point is not used by a key ring.

Procedure

Step 1 Enters security mode:

Firepower-chassis# **scope security**

Step 2 Delete the named trusted point:

Firepower-chassis /security # **delete trustpoint** *name*

Step 3 Commits the transaction:

Firepower-chassis /security # **commit-buffer**

Example

The following example deletes a trusted point:

```
Firepower-chassis# scope security
Firepower-chassis /security # delete trustpoint tPoint10
Firepower-chassis /security* # commit-buffer
Firepower-chassis /security #
```

Disabling HTTPS

Procedure

Step 1 Enter system mode:

Firepower-chassis# **scope system**

Step 2 Enter system services mode:

Firepower-chassis /system # **scope services**

Step 3 Disable the HTTPS service:

Firepower-chassis /system/services # **disable https**

Step 4 Commit the transaction to the system configuration:

Firepower-chassis /system/services # **commit-buffer**

Example

The following example disables HTTPS and commits the transaction:

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # disable https
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

Configuring AAA

This section describes authentication, authorization, and accounting. See the following topics for more information:

About AAA

Authentication, Authorization and Accounting (AAA) is a set of services for controlling access to network resources, enforcing policies, assessing usage, and providing the information necessary to bill for services. Authentication identifies the user. Authorization implements policies that determine which resources and services an authenticated user may access. Accounting keeps track of time and data resources that are used for billing and analysis. These processes are considered important for effective network management and security.

Authentication

Authentication provides a way to identify each user, typically by having the user enter a valid user name and valid password before access is granted. The AAA server compares the user's provided credentials with user credentials stored in a database. If the credentials are matched, the user is permitted access to the network. If the credentials do not match, authentication fails and network access is denied.

You can configure the Firepower 9300 chassis to authenticate administrative connections to the chassis, including the following sessions:

- HTTPS
- SSH
- Serial console

Authorization

Authorization is the process of enforcing policies: determining what types of activities, resources, or services each user is permitted to access. After authentication, a user may be authorized for different types of access or activity.

Accounting

Accounting measures the resources a user consumes during access, which may include the amount of system time or the amount of data that a user has sent or received during a session. Accounting is carried out through the logging of session statistics and usage information, which is used for authorization control, billing, trend analysis, resource utilization, and capacity planning activities.

Interaction Between Authentication, Authorization, and Accounting

You can use authentication alone, or with authorization and accounting. Authorization always requires a user to be authenticated first. You can use accounting alone, or with authentication and authorization.

Supported Types of Authentication

FXOS supports the following types of user Authentication:

- **Remote** – The following network AAA services are supported:
  - LDAP
  - RADIUS
  - TACACS+
- **Local** – The Firepower chassis maintains a local database that you can populate with user profiles. You can use this local database instead of AAA servers to provide user authentication, authorization, and accounting.

User Roles

FXOS supports local and remote Authorization in the form of user-role assignment. The roles that can be assigned are:

- **Admin** – Complete read-and-write access to the entire system. The default admin account is assigned this role by default and it cannot be changed.
- **AAA Administrator** – Read-and-write access to users, roles, and AAA configuration. Read access to the rest of the system.

- **Operations** – Read-and-write access to NTP configuration, Smart Call Home configuration for Smart Licensing, and system logs, including syslog servers and faults. Read access to the rest of the system.
- **Read-Only** – Read-only access to system configuration with no privileges to modify the system state.

See User Management, on page 21 for more information about local users and role assignments.

Setting Up AAA

These steps provide a basic outline for setting up Authentication, Authorization and Accounting (AAA) on a Firepower 4100/9300 appliance.

1. Configure the desired type(s) of user authentication:
    - **Local** – User definitions and local authentication are part of User Management, on page 21.
    - **Remote** – Configuring remote AAA server access is part of Platform Settings, specifically:
        - Configuring LDAP Providers, on page 68
        - Configuring RADIUS Providers, on page 72
        - Configuring TACACS+ Providers, on page 74

    Note If you will be using remote AAA servers, be sure to enable and configure AAA services on the remote servers before configuring remote AAA server access on the Firepower chassis.

2. Specify the default authentication method—this also is part of User Management, on page 21.

Note If Default Authentication and Console Authentication are both set to use the same remote authentication protocol (RADIUS, TACACS+, or LDAP), you cannot change certain aspects of that server's configuration (for example, deleting that server, or changing its order of assignment) without updating these user settings.

Configuring LDAP Providers

Configuring Properties for LDAP Providers

The properties that you configure in this task are the default settings for all provider connections of this type. If an individual provider includes a setting for any of these properties, the Firepower eXtensible Operating System uses that setting and ignores the default setting.

If you are using Active Directory as your LDAP server, create a user account in the Active Directory server to bind with the Firepower eXtensible Operating System. This account should be given a non-expiring password.

Procedure

Step 1 Choose **Platform Settings** > **AAA**.

Step 2 Click the **LDAP** tab.

Step 3 In the **Properties** area, complete the following fields:

Name	Description
Timeout field	The length of time in seconds the system will spend trying to contact the LDAP database before it times out. Enter an integer from 1 to 60 seconds. The default value is 30 seconds. This property is required.
Attribute field	An LDAP attribute that stores the values for the user roles and locales. This property is always a name-value pair. The system queries the user record for the value that matches this attribute.
Base DN field	The specific distinguished name in the LDAP hierarchy where the server should begin a search when a remote user logs in and the system attempts to get the user's DN based on their user name. The length of the base DN can be a maximum of 255 characters minus the length of *cn=$userid*, where $userid identifies the remote user attempting to access the Firepower chassis using LDAP authentication. This property is required for LDAP providers. If you do not specify a base DN on this tab, then you must specify one for each LDAP provider that you define.
Filter field	Enter the filter attribute to use with your LDAP server, for example *cn=$userid* or *sAMAccountName=$userid*. The LDAP search is restricted to those user names that match the defined filter. The filter must include *$userid*. This property is required. If you do not specify a filter on this tab then you must specify one for each LDAP provider that you define.

Step 4 Click **Save**.

What to do next

Create an LDAP provider.

Creating an LDAP Provider

Follow these steps to define and configure a LDAP provider—that is, a specific remote server providing LDAP-based AAA services for this Firepower appliance.

Note The Firepower eXtensible Operating System supports a maximum of 16 LDAP providers.

Before you begin

If you are using Active Directory as your LDAP server, create a user account in the Active Directory server to bind with the Firepower eXtensible Operating System. This account should be given a non-expiring password.

Procedure

Step 1 Choose **Platform Settings** > **AAA**.

Step 2 Click the **LDAP** tab.

Step 3 For each LDAP provider that you want to add:

a) In the **LDAP Providers** area, click **Add**.

b) In the **Add LDAP Provider** dialog box, complete the following fields:

Name	Description
Hostname/FQDN (or IP Address) field	The hostname or IP address of the LDAP server. If SSL is enabled, this field must exactly match a Common Name (CN) in the security certificate of the LDAP database.
Order field	The order in which the Firepower eXtensible Operating System uses this provider to authenticate users. Enter an integer between 1 and 16, or enter `lowest-available` or `0` (zero) if you want the Firepower eXtensible Operating System to assign the next available order based on the other providers defined in Firepower Chassis Manager or the FXOS CLI.
Bind DN field	The distinguished name (DN) for an LDAP database account that has read and search permissions for all objects under the base DN. The maximum supported string length is 255 ASCII characters.
Base DN field	The specific distinguished name in the LDAP hierarchy where the server should begin a search when a remote user logs in and the system attempts to get the user's DN based on their user name. The length of the base DN can be set to a maximum of 255 characters minus the length of CN=$userid, where $userid identifies the remote user attempting to access Firepower Chassis Manager or the FXOS CLI using LDAP authentication. This value is required unless a default base DN has been set on the **LDAP** tab.
Port field	The port through which Firepower Chassis Manager or the FXOS CLI communicates with the LDAP database. The standard port number is 389.
Enable SSL check box	If checked, encryption is required for communications with the LDAP database. If unchecked, authentication information will be sent as clear text. LDAP uses STARTTLS. This allows encrypted communication using port 389.

Name	Description
Filter field	Enter the filter attribute to use with your LDAP server, for example *cn=$userid* or *sAMAccountName=$userid*. The LDAP search is restricted to those user names that match the defined filter. The filter must include *$userid*. This value is required unless a default filter has been set on the **LDAP** tab.
Attribute field	An LDAP attribute that stores the values for the user roles and locales. This property is always a name-value pair. The system queries the user record for the value that matches this attribute name. This value is required unless a default attribute has been set on the **LDAP** tab.
Key field	The password for the LDAP database account specified in the **Bind DN** field. You can enter any standard ASCII characters except for space, § (section sign), ? (question mark), or = (equal sign).
Confirm Key field	The LDAP database password repeated for confirmation.
Timeout field	The length of time in seconds the system will spend trying to contact the LDAP database before it times out. Enter an integer from 1 to 60 seconds, or enter 0 (zero) to use the global timeout value specified on the **LDAP** tab. The default is 30 seconds.
Vendor field	This selection identifies the vendor that is providing the LDAP provider or server details: • If the LDAP provider is Microsoft Active Directory, select **MS AD**. • If the LDAP provider is not Microsoft Active Directory, select **Open LDAP**. The default is **Open LDAP**.

c) Click **OK** to close the **Add LDAP Provider** dialog box.

Step 4 Click **Save**.

Deleting an LDAP Provider

Procedure

Step 1 Choose **Platform Settings** > **AAA**.

Step 2 Click the **LDAP** tab.

Step 3 In the **LDAP Providers** area, click the **Delete** icon in the row in the table that corresponds to the LDAP Provider you want to delete.

Configuring RADIUS Providers

Configuring Properties for RADIUS Providers

The properties that you configure in this task are the default settings for all provider connections of this type. If an individual provider includes a setting for any of these properties, the Firepower eXtensible Operating System uses that setting and ignores this default setting.

Procedure

Step 1 Choose **Platform Settings** > **AAA**.

Step 2 Click the **RADIUS** tab.

Step 3 In the **Properties** area, complete the following fields:

Name	Description
Timeout field	The length of time in seconds the system will spend trying to contact the RADIUS database before it times out. Enter an integer from 1 to 60 seconds. The default value is 5 seconds. This property is required.
Retries field	The number of times to retry the connection before the request is considered to have failed.

Step 4 Click **Save**.

What to do next

Create a RADIUS provider.

Creating a RADIUS Provider

Follow these steps to define and configure a RADIUS provider—that is, a specific remote server providing RADIUS-based AAA services for this Firepower appliance.

Note The Firepower eXtensible Operating System supports a maximum of 16 RADIUS providers.

Procedure

Step 1 Choose **Platform Settings** > **AAA**.

Step 2 Click the **RADIUS** tab.

Step 3 For each RADIUS provider that you want to add:

a) In the **RADIUS Providers** area, click **Add**.

b) In the **Add RADIUS Provider** dialog box, complete the following fields:

Name	Description
Hostname/FQDN (or IP Address) field	The hostname or IP address of the RADIUS server.
Order field	The order in which the Firepower eXtensible Operating System uses this provider to authenticate users. Enter an integer between 1 and 16, or enter `lowest-available` or `0` (zero) if you want the Firepower eXtensible Operating System to assign the next available order based on the other providers defined in Firepower Chassis Manager or the FXOS CLI.
Key field	The SSL encryption key for the database. You can enter any standard ASCII characters except for space, § (section sign), ? (question mark), or = (equal sign).
Confirm Key field	The SSL encryption key repeated for confirmation.
Authorization Port field	The port through which Firepower Chassis Manager or the FXOS CLI communicates with the RADIUS database. The valid range is 1 to 65535. The standard port number is 1700.
Timeout field	The length of time in seconds the system will spend trying to contact the RADIUS database before it times out. Enter an integer from 1 to 60 seconds, or enter 0 (zero) to use the global timeout value specified on the **RADIUS** tab. The default is 5 seconds.
Retries field	The number of times to retry the connection before the request is considered to have failed. If desired, enter an integer between 0 and 5. If you do not specify a value, Firepower Chassis Manager uses the value specified on the **RADIUS** tab.

c) Click **OK** to close the **Add RADIUS Provider** dialog box.

Step 4 Click **Save**.

Deleting a RADIUS Provider

Procedure

Step 1 Choose **Platform Settings** > **AAA**.

Step 2 Click the **RADIUS** tab.

Step 3 In the **RADIUS Providers** area, click the **Delete** icon in the row in the table that corresponds to the RADIUS Provider you want to delete.

Configuring TACACS+ Providers

Configuring Properties for TACACS+ Providers

The properties that you configure in this task are default settings for all provider connections of this type. If an individual provider configuration includes a setting for any of these properties, the Firepower eXtensible Operating System uses that setting and ignores this default setting.

Procedure

Step 1 Choose **Platform Settings** > **AAA**.

Step 2 Click the **TACACS** tab.

Step 3 In the **Properties** area, complete the following fields:

Name	Description
Timeout field	The length of time in seconds the system will spend trying to contact the TACACS+ database before it times out. Enter an integer from 1 to 60 seconds. The default value is 5 seconds. This property is required.

Step 4 Click **Save**.

What to do next

Create a TACACS+ provider.

Creating a TACACS+ Provider

Follow these steps to define and configure a TACACS+ provider—that is, a specific remote server providing TACACS-based AAA services for this Firepower appliance.

Note The Firepower eXtensible Operating System supports a maximum of 16 TACACS+ providers.

Procedure

Step 1 Choose **Platform Settings** > **AAA**.

Step 2 Click the **TACACS** tab.

Step 3 For each TACACS+ provider that you want to add:

a) In the **TACACS Providers** area, click **Add**.

b) In the **Add TACACS Provider** dialog box, complete the following fields:

Name	Description
Hostname/FQDN (or IP Address) field	The hostname or IP address of the TACACS+ server.
Order field	The order in which the Firepower eXtensible Operating System uses this provider to authenticate users. Enter an integer between 1 and 16, or enter `lowest-available` or `0` (zero) if you want the Firepower eXtensible Operating System to assign the next available order based on the other providers defined in Firepower Chassis Manager or the FXOS CLI.
Key field	The SSL encryption key for the database. You can enter any standard ASCII characters except for space, § (section sign), ? (question mark), or = (equal sign).
Confirm Key field	The SSL encryption key repeated for confirmation.
Port field	The port through which Firepower Chassis Manager or the FXOS CLI communicates with this TACACS+ server. Enter an integer between 1 and 65535. The default port is 49.
Timeout field	The length of time in seconds the system will spend trying to contact the TACACS+ database before it times out. Enter an integer from 1 to 60 seconds, or enter 0 (zero) to use the global timeout value specified on the **TACACS+** tab. The default is 5 seconds.

c) Click **OK** to close the **Add TACACS Provider** dialog box.

Step 4 Click **Save**.

Deleting a TACACS+ Provider

Procedure

Step 1 Choose **Platform Settings** > **AAA**.

Step 2 Click the **TACACS** tab.

Step 3 In the **TACACS Providers** area, click the **Delete** icon in the row in the table that corresponds to the TACACS+ Provider you want to delete.

Configuring Syslog

System logging is a method of collecting messages from devices to a server running a syslog daemon. Logging to a central syslog server helps in aggregation of logs and alerts. A syslog service accepts messages and stores them in files, or prints them according to a simple configuration file. This form of logging provides protected long-term storage for logs. Logs are useful both in routine troubleshooting and in incident handling.

Procedure

Step 1 Choose **Platform Settings** > **Syslog**.

Step 2 Configure Local Destinations:

a) Click the **Local Destinations** tab.

b) On the **Local Destinations** tab, complete the following fields:

Name	Description
Console Section	
Admin State field	Whether the Firepower chassis displays syslog messages on the console. Check the **Enable** check box if you want to have syslog messages displayed on the console as well as added to the log. If the **Enable** check box is unchecked, syslog messages are added to the log but are not displayed on the console.
Level field	If you checked the **Enable** check box for **Console - Admin State**, select the lowest message level that you want displayed on the console. The Firepower chassis displays that level and above on the console. This can be one of the following: • **Emergencies** • **Alerts** • **Critical**
Monitor Section	
Admin State field	Whether the Firepower chassis displays syslog messages on the monitor. Check the **Enable** check box if you want to have syslog messages displayed on the monitor as well as added to the log. If the **Enable** check box is unchecked, syslog messages are added to the log but are not displayed on the monitor.

Name	Description
Level drop-down list	If you checked the **Enable** check box for **Monitor - Admin State**, select the lowest message level that you want displayed on the monitor. The system displays that level and above on the monitor. This can be one of the following: • **Emergencies** • **Alerts** • **Critical** • **Errors** • **Warnings** • **Notifications** • **Information** • **Debugging**

c) Click **Save**.

Step 3 Configure Remote Destinations:

a) Click the **Remote Destinations** tab.
b) On the **Remote Destinations** tab, complete the following fields for up to three external logs that can store messages generated by the Firepower chassis:

By sending syslog messages to a remote destination, you can archive messages according to the available disk space on the external syslog server, and manipulate logging data after it is saved. For example, you could specify actions to be executed when certain types of syslog messages are logged, extract data from the log and save the records to another file for reporting, or track statistics using a site-specific script.

Name	Description
Admin State field	Check the **Enable** check box if you want to have syslog messages stored in a remote log file.
Level drop-down list	Select the lowest message level that you want the system to store. The system stores that level and above in the remote file. This can be one of the following: • **Emergencies** • **Alerts** • **Critical** • **Errors** • **Warnings** • **Notifications** • **Information** • **Debugging**

Name	Description
Hostname/IP Address field	The hostname or IP address on which the remote log file resides. **Note** You must configure a DNS server if you use a hostname rather than an IP address.
Facility drop-down list	Choose a system log facility for syslog servers to use as a basis to file messages. This can be one of the following: • **Local0** • **Local1** • **Local2** • **Local3** • **Local4** • **Local5** • **Local6** • **Local7**

c) Click **Save**.

Step 4 Configure Local Sources:

a) Click the **Local Sources** tab.
b) On the **Local Sources** tab, complete the following fields:

Name	Description
Faults Admin State field	Whether system fault logging is enabled or not. If the **Enable** check box is checked, the Firepower chassis logs all system faults.
Audits Admin State field	Whether audit logging is enabled or not. If the **Enable** check box is checked, the Firepower chassis logs all audit log events.
Events Admin State field	Whether system event logging is enabled or not. If the **Enable** check box is checked, the Firepower chassis logs all system events.

c) Click **Save**.

Configuring DNS Servers

You need to specify a DNS server if the system requires resolution of host names to IP addresses. For example, you cannot use a name such as www.cisco.com when you are configuring a setting on the Firepower chassis if you do not configure a DNS server. You would need to use the IP address of the server, which can be either an IPv4 or an IPv6 address. You can configure up to four DNS servers.

Note When you configure multiple DNS servers, the system searches for the servers only in any random order. If a local management command requires DNS server lookup, it can only search for three DNS servers in random order.

Procedure

Step 1 Choose **Platform Settings** > **DNS**.

Step 2 Check the **Enable DNS Server** check box.

Step 3 For each DNS server that you want to add, up to a maximum of four, enter the IP address of the DNS server in the **DNS Server** field and click **Add**.

Step 4 Click **Save**.

CHAPTER 7

Interface Management

About Firepower Interfaces

The Firepower 9300 chassis supports physical interfaces and EtherChannel (port-channel) interfaces. EtherChannel interfaces can include up to 16 member interfaces of the same type.

Chassis Management Interface

The chassis management interface is used for management of the FXOS Chassis by SSH or Firepower Chassis Manager. This interface appears at the top of the **Interfaces** tab as **MGMT**, and you can only enable or disable this interface on the **Interfaces** tab. This interface is separate from the mgmt-type interface that you assign to the logical devices for application management.

To configure parameters for this interface, you must configure them from the CLI. To view information about this interface in the FXOS CLI, connect to local management and show the management port:

Firepower # **connect local-mgmt**

Firepower(local-mgmt) # **show mgmt-port**

Note that the chassis management interface remains up even if the physical cable or SFP module are unplugged, or if the **mgmt-port shut** command is performed.

Interface Types

Each interface can be one of the following types:

- Data—Use for regular data. Data interfaces cannot be shared between logical devices, and logical devices cannot communicate over the backplane to other logical devices. For traffic on Data interfaces, all traffic must exit the chassis on one interface and return on another interface to reach another logical device.
- Mgmt—Use to manage application instances. These interfaces can be shared by one or more logical devices to access external hosts; logical devices cannot communicate over this interface with other logical

devices that share the interface. You can only assign one management interface per logical device. For ASA: You can later enable management from a data interface; but you must assign a Management interface to the logical device even if you don't intend to use it after you enable data management.

- Cluster—Use as the cluster control link for a clustered logical device. By default, the cluster control link is automatically created on Port-channel 48. The Cluster type is only supported on EtherChannel interfaces.

FXOS Interfaces vs. Application Interfaces

The Firepower 9300 manages the basic Ethernet settings of physical interfaces and EtherChannel (port-channel) interfaces. Within the application, you configure higher level settings. For example, you can only create EtherChannels in FXOS; but you can assign an IP address to the EtherChannel within the application.

The following sections describe the interaction between FXOS and the application for interfaces.

VLAN Subinterfaces

For all logical devices, you can create VLAN subinterfaces within the application.

Independent Interface States in the Chassis and in the Application

You can administratively enable and disable interfaces in both the chassis and in the application. For an interface to be operational, the interface must be enabled in both operating systems. Because the interface state is controlled independently, you may have a mismatch between the chassis and application.

Jumbo Frame Support

The Firepower 9300 chassis has support for jumbo frames enabled by default. To enable jumbo frame support on a specific logical device installed on the Firepower 9300 chassis, you will need to configure the appropriate MTU settings for the interfaces on the logical device.

The maximum MTU that is supported for the application on the Firepower 9300 chassis is 9000.

Guidelines and Limitations for Firepower Interfaces

Default MAC Addresses

Default MAC address assignments depend on the type of interface.

- Physical interfaces—The physical interface uses the burned-in MAC address.

- EtherChannels—For an EtherChannel, all interfaces that are part of the channel group share the same MAC address. This feature makes the EtherChannel transparent to network applications and users, because they only see the one logical connection; they have no knowledge of the individual links. The port-channel interface uses a unique MAC address from a pool; interface membership does not affect the MAC address.

Configure Interfaces

By default, physical interfaces are disabled. You can enable interfaces, add EtherChannels, and edit interface properties.

Enable or Disable an Interface

You can change the **Admin State** of each interface to be enabled or disabled. By default, physical interfaces are disabled.

Procedure

Step 1 Choose **Interfaces** to open the Interfaces page.

The Interfaces page shows a visual representation of the currently installed interfaces at the top of the page and provides a listing of the installed interfaces in the table below.

Step 2 To enable the interface, click the disabled **Slider disabled** ( ) so that it changes to the enabled **Slider enabled** ( ).

Click **Yes** to confirm the change. The corresponding interface in the visual representation changes from gray to green.

Step 3 To disable the interface, click the enbled **Slider enabled** ( ) so that it changes to the disabled **Slider disabled** ( ).

Click **Yes** to confirm the change. The corresponding interface in the visual representation changes from green to gray.

Configure a Physical Interface

You can physically enable and disable interfaces, as well as set the interface speed and duplex. To use an interface, it must be physically enabled in FXOS and logically enabled in the application.

Before you begin

- Interfaces that are already a member of an EtherChannel cannot be modified individually. Be sure to configure settings before you add it to the EtherChannel.

Procedure

Step 1 Choose **Interfaces** to open the Interfaces page.

The **All Interfaces** page shows a visual representation of the currently installed interfaces at the top of the page and provides a listing of the installed interfaces in the table below.

Step 2 Click **Edit** in the row for the interface you want to edit to open the **Edit Interface** dialog box.

Step 3 To enable the interface, check the **Enable** check box. To disable the interface, uncheck the **Enable** check box.

Step 4 Choose the interface **Type**:

- **Data**
- **Mgmt**
- **Cluster**—Do not choose the **Cluster** type; by default, the cluster control link is automatically created on Port-channel 48.

Step 5 (Optional) Choose the speed of the interface from the **Speed** drop-down list.

Step 6 (Optional) If your interface supports **Auto Negotiation**, click the **Yes** or **No** radio button.

Step 7 (Optional) Choose the duplex of the interface from the **Duplex** drop-down list.

Step 8 Click **OK**.

Add an EtherChannel (Port Channel)

An EtherChannel (also known as a port channel) can include up to 16 member interfaces of the same media type and capacity, and must be set to the same speed and duplex. The media type can be either RJ-45 or SFP; SFPs of different types (copper and fiber) can be mixed. You cannot mix interface capacities (for example 1GB and 10GB interfaces) by setting the speed to be lower on the larger-capacity interface. The Link Aggregation Control Protocol (LACP) aggregates interfaces by exchanging the Link Aggregation Control Protocol Data Units (LACPDUs) between two network devices.

LACP coordinates the automatic addition and deletion of links to the EtherChannel without user intervention. It also handles misconfigurations and checks that both ends of member interfaces are connected to the correct channel group.

When the Firepower 9300 chassis creates an EtherChannel, the EtherChannel stays in a **Suspended** state until you assign it to a logical device, even if the physical link is up. The EtherChannel will be brought out of this **Suspended** state in the following situations:

- The EtherChannel is added as a data or management interface for a standalone logical device
- The EtherChannel is added as a management interface or cluster control link for a logical device that is part of a cluster
- The EtherChannel is added as a data interface for a logical device that is part of a cluster and at least one unit has joined the cluster

Note that the EtherChannel does not come up until you assign it to a logical device. If the EtherChannel is removed from the logical device or the logical device is deleted, the EtherChannel will revert to a **Suspended** state.

Procedure

Step 1 Choose **Interfaces** to open the Interfaces page.

The **All Interfaces** page shows a visual representation of the currently installed interfaces at the top of the page and provides a listing of the installed interfaces in the table below.

Step 2 Click **Add Port Channel** above the interfaces table to open the **Add Port Channel** dialog box.

Step 3 Enter an ID for the port channel in the **Port Channel ID** field. Valid values are between 1 and 47.

Port-channel 48 is reserved for the cluster control link when you deploy a clustered logical device. If you do not want to use Port-channel 48 for the cluster control link, you can delete it and configure a Cluster type EtherChannel with a different ID. For intra-chassis clustering, do not assign any interfaces to the Cluster EtherChannel.

Step 4 To enable the port channel, check the **Enable** check box. To disable the port channel, uncheck the **Enable** check box.

Step 5 Choose the interface **Type**:

- **Data**
- **Mgmt**
- **Cluster**

Step 6 Set the **Admin Speed** of the member interfaces from the drop-down list.

Step 7 Set the **Admin Duplex**, **Full Duplex** or **Half Duplex**.

Step 8 To add an interface to the port channel, select the interface in the **Available Interface** list and click **Add Interface** to move the interface to the Member ID list. You can add up to 16 interfaces.

Tip You can add multiple interfaces at one time. To select multiple individual interfaces, click on the desired interfaces while holding down the **Ctrl** key. To select a range of interfaces, select the first interface in the range, and then, while holding down the **Shift** key, click to select the last interface in the range.

Step 9 To remove an interface from the port channel, click the **Delete** button to the right of the interface in the Member ID list.

Step 10 Click **OK**.

Configure Breakout Cables

The following procedure shows how to configure breakout cables for use with the Firepower 9300 chassis. You can use a breakout cable to provide four 10 Gbps ports in place of a single 40 Gbps port.

Procedure

Step 1 Choose **Interfaces** to open the Interfaces page.

The Interfaces page shows a visual representation of the currently installed interfaces at the top of the page and provides a listing of the installed interfaces in the table below.

The interfaces that are capable of supporting breakout cables but are not currently configured as such are indicated by a Breakout Port icon in the row for that interface. For interfaces that have already been configured as using a breakout cable, the individual breakout interfaces are listed separately (for example, Ethernet 2/1/1, 2/1/2, 2/1/3, and 2/1/4).

Step 2 To convert a 40 Gbps interface into four 10 Gbps interfaces:

a) Click the **Breakout Port** icon for the interface that you want to convert.

The Breakout Port Creation dialog box opens asking you to confirm that you want to proceed and warning you that the chassis will be rebooted.

b) Click **Yes** to confirm.

The Firepower chassis reboots and the specified interface is converted into four 10 Gbps interfaces.

Step 3 To convert the four 10 Gbps breakout interfaces back into a single 40 Gbps interface:

a) Click **Delete** for any of the breakout interfaces.

A confirmation dialog box opens asking you to confirm that you want to proceed and warning you that all four breakout interfaces will be deleted and that the chassis will be rebooted.

b) Click **Yes** to confirm.

The Firepower chassis reboots and the specified interfaces are converted into a single 40 Gbps interface.

Monitoring Interfaces

From the Interfaces page of the Firepower Chassis Manager, you can view the status of the installed interfaces on the chassis, edit interface properties, enable or disable an interface, and create port channels.

The Interfaces page is made up of two sections:

- The upper section shows a visual representation of the interfaces that are installed in the Firepower chassis. You can hover over any of the interfaces to get additional information about the interface.

  The interfaces are color coded to indicate their current status:

  - Green—The interface is installed and enabled.
  - Dark Grey—The interface is installed but disabled.
  - Red—There is a problem with the operational state of the interface.
  - Light Grey—The interface is not installed.

  Note Interfaces that act as ports in port channels do not appear in this list.

- The lower section contains a table of the interfaces installed in the Firepower chassis. For each interface, you can enable or disable the interface. You can also click **Edit** to edit the properties of an interface, such as speed and interface type.

Note The port-channel 48 cluster type interface shows the **Operation State** as **failed** if it does not include any member interfaces. For intra-chassis clustering, this EtherChannel does not require any member interfaces, and you can ignore this Operational State.

CHAPTER 8

Logical Devices

About Logical Devices

A logical device lets you run one application instance .

When you add a logical device, you also define the application instance type and version, assign interfaces, and configure bootstrap settings that are pushed to the application configuration.

Standalone and Clustered Logical Devices

You can add the following logical device types:

- Standalone—A standalone logical device operates as a standalone unit or as a unit in a High Availability pair.
- Cluster—A clustered logical device lets you group multiple units together, providing all the convenience of a single device (management, integration into a network) while achieving the increased throughput and redundancy of multiple devices. Multiple module devices, like the Firepower 9300, support intra-chassis clustering. For the Firepower 9300, all three modules must participate in the cluster.

Requirements and Prerequisites for Logical Devices

See the following sections for requirements and prerequisites.

Requirements and Prerequisites for Hardware and Software Combinations

The Firepower 9300 supports multiple models, security modules, application types, and high availability and scalability features. See the following requirements for allowed combinations.

Firepower 9300 Requirements

The Firepower 9300 includes 3 security module slots and multiple types of security modules. See the following requirements:

- Security Module Types—
- Clustering—All security modules in the cluster, whether it is intra-chassis or inter-chassis, must be the same type. You can have different quantities of installed security modules in each chassis, although all modules present in the chassis must belong to the cluster including any empty slots. For example, you can install 2 SM-36s in chassis 1, and 3 SM-36s in chassis 2.
- High Availability—High Availability is only supported between same-type modules on the Firepower 9300.
- ASA and FTD application types—
- ASA or FTD versions—You can run different versions of an application instance type on separate modules. For example, you can install FTD 6.3 on module 1, FTD 6.4 on module 2, and FTD 6.5 on module 3.

Requirements and Prerequisites for Clustering

Clustering Hardware and Software Requirements

All chassis in a cluster:

- All security modules must be the same type. For example, if you use clustering, all modules in the Firepower 9300 must be SM-40s. You can have different quantities of installed security modules in each chassis, although all modules present in the chassis must belong to the cluster including any empty slots.
- Must run the identical FXOS software except at the time of an image upgrade.
- Must include the same interface configuration for interfaces you assign to the cluster, such as the same Management interface, EtherChannels, active interfaces, speed and duplex, and so on. You can use different network module types on the chassis as long as the capacity matches for the same interface IDs and interfaces can successfully bundle in the same spanned EtherChannel. Note that all data interfaces must be EtherChannels in inter-chassis clustering. If you change the interfaces in FXOS after you enable clustering (by adding or removing interface modules, or configuring EtherChannels, for example), then perform the same changes on each chassis, starting with the data units, and ending with the control unit.
- Must use the same NTP server. Do not set the time manually.
- ASA: Each FXOS chassis must be registered with the License Authority or satellite server. There is no extra cost for data units. For Firepower Threat Defense, all licensing is handled by the Firepower Management Center.

Switch Requirements for Inter-Chassis Clustering

- Be sure to complete the switch configuration and successfully connect all the EtherChannels from the chassis to the switch(es) before you configure clustering on the Firepower 9300 chassis.
- For supported switch characteristics, see Cisco FXOS Compatibility.

Sizing the Data Center Interconnect for Inter-Site Clustering

You should reserve bandwidth on the data center interconnect (DCI) for cluster control link traffic equivalent to the following calculation:

$$\frac{\text{\# of cluster members per site}}{2} \times \text{cluster control link size per member}$$

If the number of members differs at each site, use the larger number for your calculation. The minimum bandwidth for the DCI should not be less than the size of the cluster control link for one member.

For example:

- For 4 members at 2 sites:
  - 4 cluster members total
  - 2 members at each site
  - 5 Gbps cluster control link per member

  Reserved DCI bandwidth = 5 Gbps (2/2 x 5 Gbps).
- For 6 members at 3 sites, the size increases:
  - 6 cluster members total
  - 3 members at site 1, 2 members at site 2, and 1 member at site 3
  - 10 Gbps cluster control link per member

  Reserved DCI bandwidth = 15 Gbps (3/2 x 10 Gbps).
- For 2 members at 2 sites:
  - 2 cluster members total
  - 1 member at each site
  - 10 Gbps cluster control link per member

  Reserved DCI bandwidth = 10 Gbps (1/2 x 10 Gbps = 5 Gbps; but the minimum bandwidth should not be less than the size of the cluster control link (10 Gbps)).

Requirements and Prerequisites for High Availability

- The two units in a High Availability Failover configuration must:
  - Be on a separate chassis; intra-chassis High Availability for the Firepower 9300 is not supported.

  - Be the same model.
  - Have the same interfaces assigned to the High Availability logical devices.
  - Have the same number and types of interfaces. All interfaces must be preconfigured in FXOS identically before you enable High Availability.

- For High Availability system requirements, see.

Guidelines and Limitations for Logical Devices

See the following sections for guidelines and limitations.

General Guidelines and Limitations

Firewall Mode

You can set the firewall mode to routed or transparent in the bootstrap configuration for the FTD.

High Availability

- Configure high availability within the application configuration.
- You can use any data interfaces as the failover and state links.

Context Mode

- Multiple context mode is only supported on the ASA.

Clustering Guidelines and Limitations

Switches for Inter-Chassis Clustering

- For the ASR 9006, if you want to set a non-default MTU, set the ASR interface MTU to be 14 bytes higher than the cluster device MTU. Otherwise, OSPF adjacency peering attempts may fail unless the **mtu-ignore** option is used. Note that the cluster device MTU should match the ASR *IPv4* MTU.
- On the switch(es) for the cluster control link interfaces, you can optionally enable Spanning Tree PortFast on the switch ports connected to the cluster unit to speed up the join process for new units.
- On the switch, we recommend that you use one of the following EtherChannel load-balancing algorithms: **source-dest-ip** or **source-dest-ip-port** (see the Cisco Nexus OS and Cisco IOS **port-channel load-balance** command). Do not use a **vlan** keyword in the load-balance algorithm because it can cause unevenly distributed traffic to the devices in a cluster.
- If you change the load-balancing algorithm of the EtherChannel on the switch, the EtherChannel interface on the switch temporarily stops forwarding traffic, and the Spanning Tree Protocol restarts. There will be a delay before traffic starts flowing again.

- Some switches do not support dynamic port priority with LACP (active and standby links). You can disable dynamic port priority to provide better compatibility with Spanned EtherChannels.
- Switches on the cluster control link path should not verify the L4 checksum. Redirected traffic over the cluster control link does not have a correct L4 checksum. Switches that verify the L4 checksum could cause traffic to be dropped.
- Port-channel bundling downtime should not exceed the configured keepalive interval.
- On Supervisor 2T EtherChannels, the default hash distribution algorithm is adaptive. To avoid asymmetric traffic in a VSS design, change the hash algorithm on the port-channel connected to the cluster device to fixed:

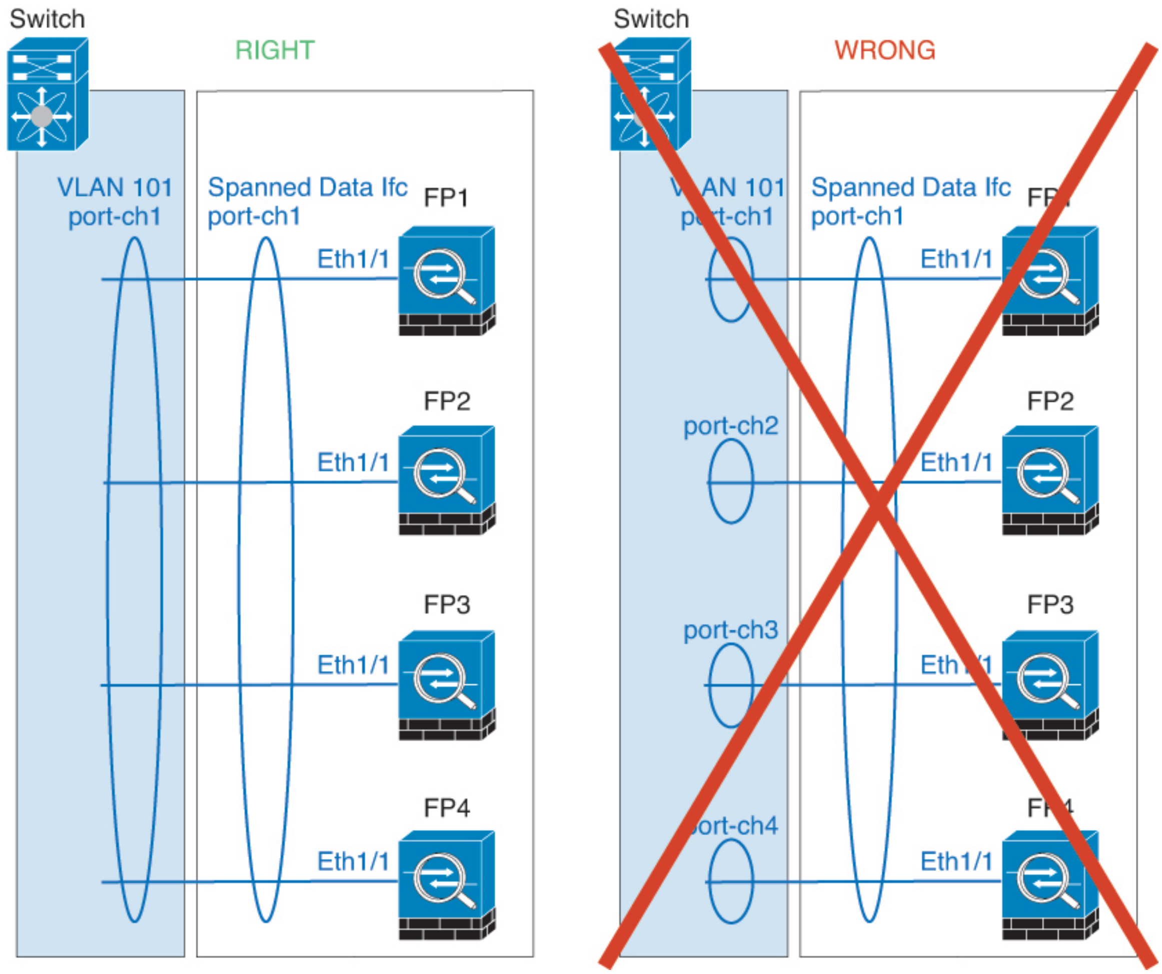
  router(config)# **port-channel** *id* **hash-distribution fixed**

  Do not change the algorithm globally; you may want to take advantage of the adaptive algorithm for the VSS peer link.

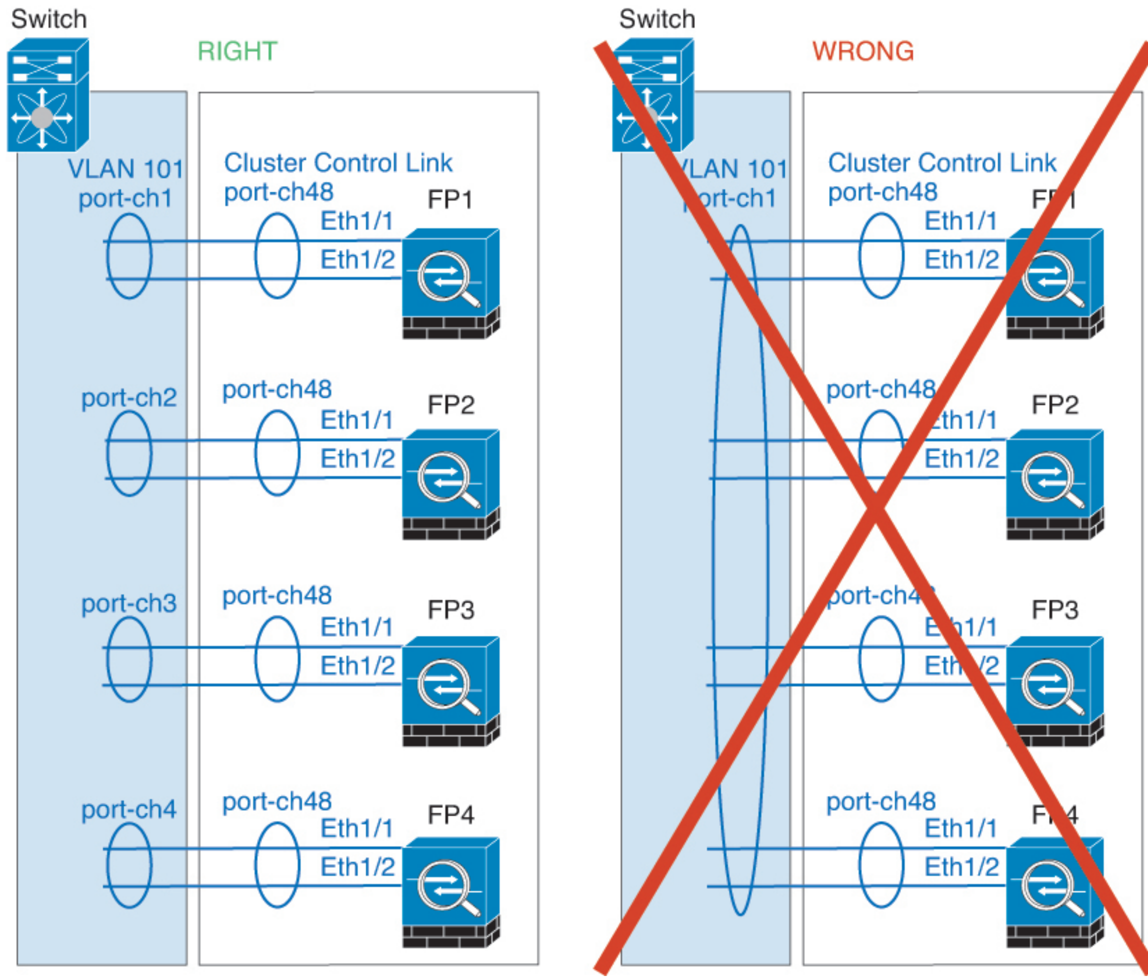
- Firepower 4100/9300 clusters support LACP graceful convergence. So you can leave LACP graceful convergence enabled on connected Cisco Nexus switches.
- When you see slow bundling of a Spanned EtherChannel on the switch, you can enable LACP rate fast for an individual interface on the switch. FXOS EtherChannels have the LACP rate set to fast by default. Note that some switches, such as the Nexus series, do not support LACP rate fast when performing in-service software upgrades (ISSUs), so we do not recommend using ISSUs with clustering.

EtherChannels for Inter-Chassis Clustering

- In Catalyst 3750-X Cisco IOS software versions earlier than 15.1(1)S2, the cluster unit did not support connecting an EtherChannel to a switch stack. With default switch settings, if the cluster unit EtherChannel is connected cross stack, and if the control unit switch is powered down, then the EtherChannel connected to the remaining switch will not come up. To improve compatibility, set the **stack-mac persistent timer** command to a large enough value to account for reload time; for example, 8 minutes or 0 for indefinite. Or, you can upgrade to more a more stable switch software version, such as 15.1(1)S2.
- Spanned vs. Device-Local EtherChannel Configuration—Be sure to configure the switch appropriately for Spanned EtherChannels vs. Device-local EtherChannels.
  - Spanned EtherChannels—For cluster unit *Spanned* EtherChannels, which span across all members of the cluster, the interfaces are combined into a single EtherChannel on the switch. Make sure each interface is in the same channel group on the switch.



- Device-local EtherChannels—For cluster unit *Device-local* EtherChannels including any EtherChannels configured for the cluster control link, be sure to configure discrete EtherChannels on the switch; do not combine multiple cluster unit EtherChannels into one EtherChannel on the switch.



Inter-Site Clustering

See the following guidelines for inter-site clustering:

- The cluster control link latency must be less than 20 ms round-trip time (RTT).
- The cluster control link must be reliable, with no out-of-order or dropped packets; for example, you should use a dedicated link.
- Do not configure connection rebalancing; you do not want connections rebalanced to cluster members at a different site.
- The cluster implementation does not differentiate between members at multiple sites for incoming connections; therefore, connection roles for a given connection may span across sites. This is expected behavior.
- For transparent mode, if the cluster is placed between a pair of inside and outside routers (AKA North-South insertion), you must ensure that both inside routers share a MAC address, and also that both outside routers share a MAC address. When a cluster member at site 1 forwards a connection to a member at site 2, the destination MAC address is preserved. The packet will only reach the router at site 2 if the MAC address is the same as the router at site 1.

- For transparent mode, if the cluster is placed between data networks and the gateway router at each site for firewalling between internal networks (AKA East-West insertion), then each gateway router should use a First Hop Redundancy Protocol (FHRP) such as HSRP to provide identical virtual IP and MAC address destinations at each site. The data VLANs are extended across the sites using Overlay Transport Virtualization (OTV), or something similar. You need to create filters to prevent traffic that is destined to the local gateway router from being sent over the DCI to the other site. If the gateway router becomes unreachable at one site, you need to remove any filters so traffic can successfully reach the other site's gateway.
- For routed mode using Spanned EtherChannel, configure site-specific MAC addresses. Extend the data VLANs across the sites using OTV, or something similar. You need to create filters to prevent traffic that is destined to the global MAC address from being sent over the DCI to the other site. If the cluster becomes unreachable at one site, you need to remove any filters so traffic can successfully reach the other site's cluster units. Dynamic routing is not supported when an inter-site cluster acts as the first hop router for an extended segment.

Additional Guidelines

- When adding a unit to an existing cluster, or when reloading a unit, there will be a temporary, limited packet/connection drop; this is expected behavior. In some cases, the dropped packets can hang connections; for example, dropping a FIN/ACK packet for an FTP connection will make the FTP client hang. In this case, you need to reestablish the FTP connection.
- If you use a Windows 2003 server connected to a Spanned EtherChannel interface, when the syslog server port is down, and the server does not throttle ICMP error messages, then large numbers of ICMP messages are sent back to the cluster. These messages can result in some units of the cluster experiencing high CPU, which can affect performance. We recommend that you throttle ICMP error messages.
- We recommend connecting EtherChannels to a VSS or vPC for redundancy.
- Within a chassis, you cannot cluster some security modules and run other security modules in standalone mode; you must include all security modules in the cluster.

Defaults

- The cluster health check feature is enabled by default with the holdtime of 3 seconds. Interface health monitoring is enabled on all interfaces by default.
- The cluster auto-rejoin feature for a failed cluster control link is set to unlimited attempts every 5 minutes.
- The cluster auto-rejoin feature for a failed data interface is set to 3 attempts every 5 minutes, with the increasing interval set to 2.
- Connection replication delay of 5 seconds is enabled by default for HTTP traffic.

Add a Standalone Logical Device

Standalone logical devices can be used alone or as high availability units. For more information about high availability usage, see Add a High Availability Pair, on page 98.

Add a Standalone ASA

Standalone logical devices work either alone or in a High Availability pair. On the Firepower 9300 with multiple security modules, you can deploy either a cluster or standalone devices. The cluster must use all modules, so you cannot mix and match a 2-module cluster plus a single standalone device, for example.

You can deploy a routed firewall mode ASA from the Firepower 9300 chassis.

For multiple context mode, you must first deploy the logical device, and then enable multiple context mode in the ASA application.

Before you begin

- Download the application image you want to use for the logical device from Cisco.com, and then upload that image to the Firepower 9300 chassis.
- Configure a management interface to use with the logical device. The management interface is required. Note that this management interface is not the same as the chassis management port that is used only for chassis management (and that appears at the top of the **Interfaces** tab as **MGMT**).
- Gather the following information:
  - Interface IDs for this device
  - Management interface IP address and network mask
  - Gateway IP address

Procedure

Step 1 Choose **Logical Devices**.

Step 2 Click , and set the following parameters:

a) Provide a **Device Name**.

   This name is used by the chassis supervisor to configure management settings and to assign interfaces; it is not the device name used in the application configuration.

b) For the **Template**, choose **Cisco: Adaptive Security Appliance**.

c) Choose the **Image Version**.

d) Click **OK**.

   You see the Provisioning - *device name* window.

Step 3 Expand the **Data Ports** area, and click each port that you want to assign to the device.

You can only assign data interfaces that you previously enabled on the **Interfaces** page. You will later enable and configure these interfaces on the ASA, including setting the IP addresses.

Step 4 Click the device icon in the center of the screen.

A dialog box appears where you can configure initial bootstrap settings. These settings are meant for initial deployment only, or for disaster recovery. For normal operation, you can later change most values in the application CLI configuration.

Step 5 On the **General Information** page, complete the following:

a) (For the Firepower 9300) Under **Security Module Selection** click the security module that you want to use for this logical device.

b) Choose the **Management Interface**.

This interface is used to manage the logical device. This interface is separate from the chassis management port.

c) Choose the management interface **Address Type**: **IPv4 only**, **IPv6 only**, or **IPv4 and IPv6**.

d) Configure the **Management IP** address.

Set a unique IP address for this interface.

e) Enter a **Network Mask** or **Prefix Length**.

f) Enter a **Network Gateway** address.

Step 6 Click the **Settings** tab.

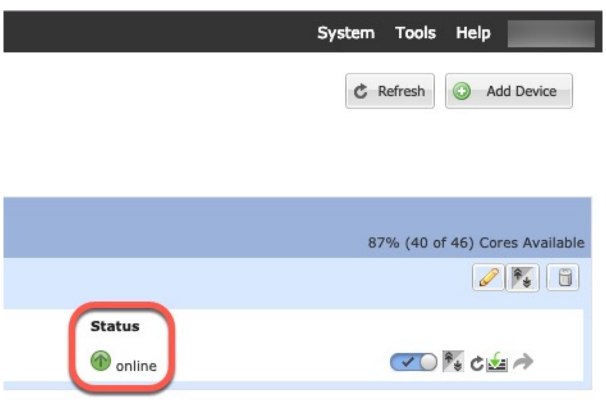
Step 7 Enter and confirm a **Password** for the admin user.

The pre-configured ASA admin user/password is useful for password recovery; if you have FXOS access, you can reset the admin user password if you forget it.

Step 8 Click **OK** to close the configuration dialog box.

Step 9 Click **Save**.

The chassis deploys the logical device by downloading the specified software version and pushing the bootstrap configuration and management interface settings to the application instance. Check the **Logical Devices** page for the status of the new logical device. When the logical device shows its **Status** as **online**, you can start configuring the security policy in the application.



Step 10 See the ASA configuration guide to start configuring your security policy.

Add a High Availability Pair

High Availability (also known as failover) is configured within the application, not in FXOS. However, to prepare your chassis for high availability, see the following steps.

Before you begin

See .

Procedure

Step 1 Allocate the same interfaces to each logical device.

Step 2 Allocate 1 or 2 data interfaces for the failover and state link(s).

These interfaces exchange high availability traffic between the 2 chassis. We recommend that you use a 10 GB data interface for a combined failover and state link. If you have available interfaces, you can use separate failover and state links; the state link requires the most bandwidth. You cannot use the management-type interface for the failover or state link. We recommend that you use a switch between the chassis, with no other device on the same network segment as the failover interfaces.

Step 3 Enable High Availability on the logical devices.

Step 4 If you need to make interface changes after you enable High Availability, perform the changes on the standby unit first, and then perform the changes on the active unit.

Add a Cluster

Clustering lets you group multiple devices together as a single logical device. A cluster provides all the convenience of a single device (management, integration into a network) while achieving the increased throughput and redundancy of multiple devices. The Firepower 9300, which includes multiple modules, supports intra-chassis clustering where you group all modules within a single chassis into a cluster. You can also use inter-chassis clustering, where multiple chassis are grouped together.

Note The FTD does not support a cluster across multiple chassis (inter-chassis); only intra-chassis clustering is supported.

About Clustering on the Firepower 9300 Chassis

The cluster consists of multiple devices acting as a single logical unit. When you deploy a cluster on the Firepower 9300 chassis, it does the following:

- Creates a *cluster-control link* (by default, port-channel 48) for unit-to-unit communication.

  For intra-chassis clustering, this link utilizes the Firepower 9300 backplane for cluster communications.

  For inter-chassis clustering, you need to manually assign physical interface(s) to this EtherChannel for communications between chassis.

- Creates the cluster bootstrap configuration within the application.

  When you deploy the cluster, the chassis supervisor pushes a minimal bootstrap configuration to each unit that includes the cluster name, cluster control link interface, and other cluster settings. Some parts of the bootstrap configuration may be user-configurable within the application if you want to customize your clustering environment.

- Assigns data interfaces to the cluster as *Spanned* interfaces.

  For intra-chassis clustering, spanned interfaces are not limited to EtherChannels, like it is for inter-chassis clustering.The Firepower 9300 supervisor uses EtherChannel technology internally to load-balance traffic to multiple modules on a shared interface, so any data interface type works for Spanned mode. For inter-chassis clustering, you must use Spanned EtherChannels for all data interfaces.

  Note Individual interfaces are not supported, with the exception of a management interface.

- Assigns a management interface to all units in the cluster.

The following sections provide more detail about clustering concepts and implementation.

Primary and Secondary Unit Roles

One member of the cluster is the primary unit. The primary unit is determined automatically. All other members are secondary units.

You must perform all configuration on the primary unit only; the configuration is then replicated to the secondary units.

Cluster Control Link

The cluster control link is automatically created using the Port-channel 48 interface.

For intra-chassis clustering, this interface has no member interfaces. This Cluster type EtherChannel utilizes the Firepower 9300 backplane for cluster communications for intra-chassis clustering. For inter-chassis clustering, you must add one or more interfaces to the EtherChannel.

For a 2-member inter-chassis cluster, do not directly connect the cluster control link from one chassis to the other chassis. If you directly connect the interfaces, then when one unit fails, the cluster control link fails, and thus the remaining healthy unit fails. If you connect the cluster control link through a switch, then the cluster control link remains up for the healthy unit.

Cluster control link traffic includes both control and data traffic.

Size the Cluster Control Link for Inter-Chassis Clustering

If possible, you should size the cluster control link to match the expected throughput of each chassis so the cluster-control link can handle the worst-case scenarios.

Cluster control link traffic is comprised mainly of state update and forwarded packets. The amount of traffic at any given time on the cluster control link varies. The amount of forwarded traffic depends on the load-balancing efficacy or whether there is a lot of traffic for centralized features. For example:

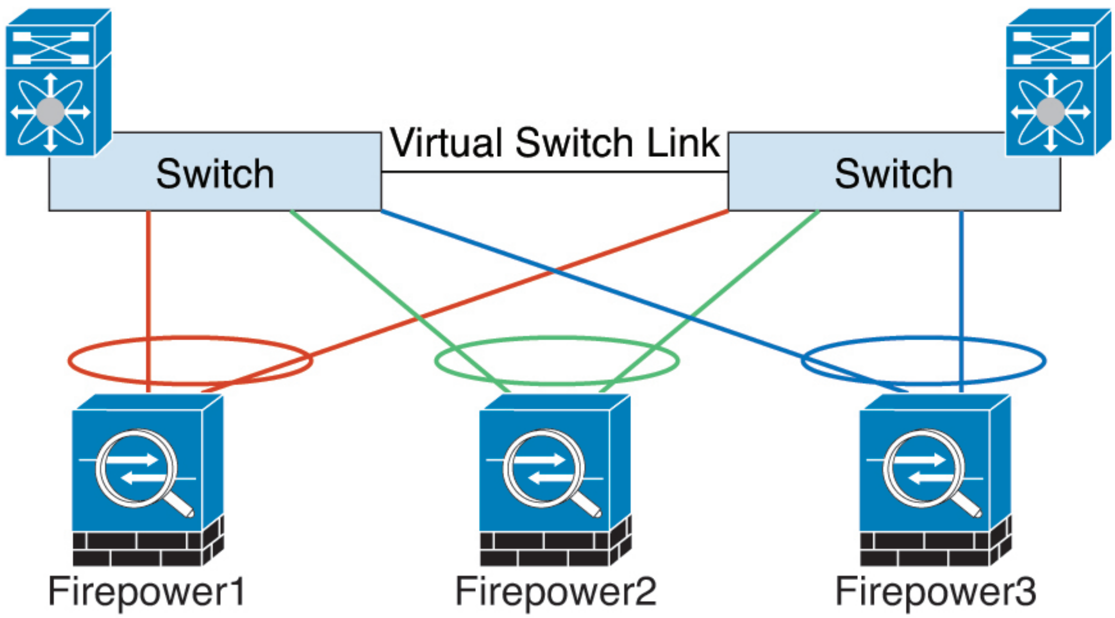
- NAT results in poor load balancing of connections, and the need to rebalance all returning traffic to the correct units.
- When membership changes, the cluster needs to rebalance a large number of connections, thus temporarily using a large amount of cluster control link bandwidth.

A higher-bandwidth cluster control link helps the cluster to converge faster when there are membership changes and prevents throughput bottlenecks.

Note If your cluster has large amounts of asymmetric (rebalanced) traffic, then you should increase the cluster control link size.

Cluster Control Link Redundancy for Inter-Chassis Clustering

The following diagram shows how to use an EtherChannel as a cluster control link in a Virtual Switching System (VSS) or Virtual Port Channel (vPC) environment. All links in the EtherChannel are active. When the switch is part of a VSS or vPC, then you can connect Firepower 9300 chassis interfaces within the same EtherChannel to separate switches in the VSS or vPC. The switch interfaces are members of the same EtherChannel port-channel interface, because the separate switches act like a single switch. Note that this EtherChannel is device-local, not a Spanned EtherChannel.



Cluster Control Link Reliability for Inter-Chassis Clustering

To ensure cluster control link functionality, be sure the round-trip time (RTT) between units is less than 20 ms. This maximum latency enhances compatibility with cluster members installed at different geographical sites. To check your latency, perform a ping on the cluster control link between units.

The cluster control link must be reliable, with no out-of-order or dropped packets; for example, for inter-site deployment, you should use a dedicated link.

Cluster Control Link Network

The Firepower 9300 chassis auto-generates the cluster control link interface IP address for each unit based on the chassis ID and slot ID: 127.2.*chassis_id*.*slot_id*. The cluster control link network cannot include any routers between units; only Layer 2 switching is allowed. For inter-site traffic, Cisco recommends using Overlay Transport Virtualization (OTV).

Management Network

We recommend connecting all units to a single management network. This network is separate from the cluster control link.

Management Interface

You must assign a Management type interface to the cluster. This interface is a special *individual* interface as opposed to a Spanned interface. The management interface lets you connect directly to each unit.

For the ASA, the Main cluster IP address is a fixed address for the cluster that always belongs to the current primary unit. You must configure a range of addresses so that each unit, including the current primary unit, can use a Local address from the range. The Main cluster IP address provides consistent management access to an address; when a primary unit changes, the Main cluster IP address moves to the new primary unit, so management of the cluster continues seamlessly. The Local IP address is used for routing, and is also useful for troubleshooting. For example, you can manage the cluster by connecting to the Main cluster IP address, which is always attached to the current primary unit. To manage an individual member, you can connect to the Local IP address. For outbound management traffic such as TFTP or syslog, each unit, including the primary unit, uses the Local IP address to connect to the server.

Spanned EtherChannels

You can group one or more interfaces per chassis into an EtherChannel that spans all chassis in the cluster. The EtherChannel aggregates the traffic across all the available active interfaces in the channel. A Spanned EtherChannel can be configured in both routed and transparent firewall modes. In routed mode, the EtherChannel is configured as a routed interface with a single IP address. In transparent mode, the IP address is assigned to the BVI, not to the bridge group member interface. The EtherChannel inherently provides load balancing as part of basic operation.

Inter-Site Clustering

For inter-site installations, you can take advantage of clustering as long as you follow the recommended guidelines.

You can configure each cluster chassis to belong to a separate site ID.

Site IDs work with site-specific MAC addresses. Packets sourced from the cluster use a site-specific MAC address, while packets received by the cluster use a global MAC address. This feature prevents the switches from learning the same global MAC address from both sites on two different ports, which causes MAC flapping; instead, they only learn the site MAC address. Site-specific MAC addresses are supported for routed mode using Spanned EtherChannels only.

Site IDs are also used to enable flow mobility using LISP inspection.

See the following sections for more information about inter-site clustering:

- Sizing the Data Center Interconnect—Requirements and Prerequisites for Clustering, on page 90
- Inter-Site Guidelines—Clustering Guidelines and Limitations, on page 92
- Inter-Site Examples—Examples for Inter-Site Clustering, on page 118

Add an ASA Cluster

You can add a single Firepower 9300 chassis as an intra-chassis cluster, or add multiple chassis for inter-chassis clustering. For inter-chassis clustering, you must configure each chassis separately. Add the cluster on one chassis; you can then copy the bootstrap configuration from the first chassis to the next chassis for ease of deployment

Create an ASA Cluster

Set the scope to the image version.

You can easily deploy the cluster from the Firepower 9300 chassis supervisor. All initial configuration is automatically generated for each unit.

For inter-chassis clustering, you must configure each chassis separately. Deploy the cluster on one chassis; you can then copy the bootstrap configuration from the first chassis to the next chassis for ease of deployment.

In a Firepower 9300 chassis, you must enable clustering for all 3 module slots, even if you do not have a module installed. If you do not configure all 3 modules, the cluster will not come up.

For multiple context mode, you must first deploy the logical device, and then enable multiple context mode in the ASA application.

Before you begin

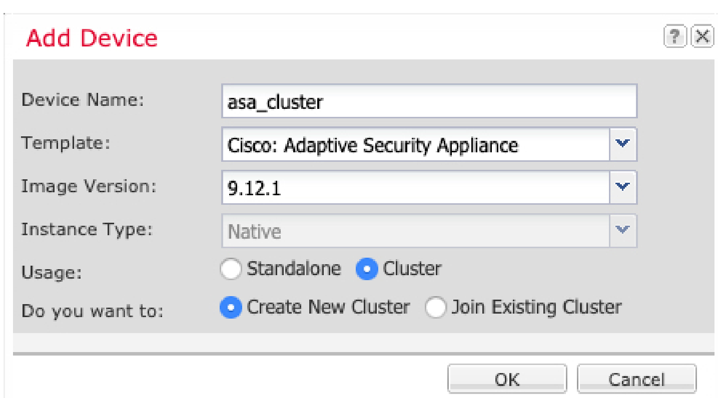
- Download the application image you want to use for the logical device from Cisco.com, and then upload that image to the Firepower 9300 chassis.
- Gather the following information:
  - Management interface ID, IP address, and network mask
  - Gateway IP address

Procedure

Step 1 Configure interfaces.

Step 2 Choose **Logical Devices**.

Step 3 Click , and set the following parameters:



a) Provide a **Device Name**.

This name is used internally by the chassis supervisor to configure management settings and to assign interfaces; it is not the device name used in the application configuration.

b) For the **Template**, choose **Cisco Adaptive Security Appliance**.
c) Choose the **Image Version**.
d) For the **Instance Type**, only the **Native** type is supported.
e) Click the **Create New Cluster** radio button.
f) Click **OK**.

You see the Provisioning - *device name* window.

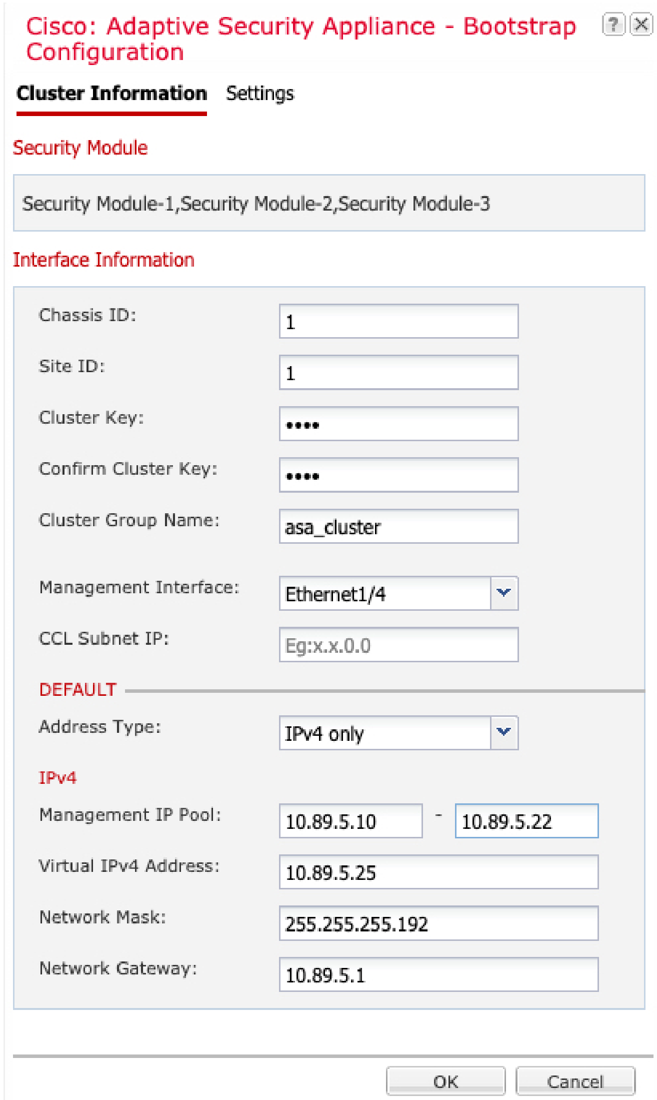
Step 4 Choose the interfaces you want to assign to this cluster.

All valid interfaces are assigned by default.

Step 5 Click the device icon in the center of the screen.

A dialog box appears where you can configure initial bootstrap settings. These settings are meant for initial deployment only, or for disaster recovery. For normal operation, you can later change most values in the application CLI configuration.

Step 6 On the **Cluster Information** page, complete the following.



a) For inter-chassis clustering, in the **Chassis ID** field, enter a chassis ID. Each chassis in the cluster must use a unique ID.

   This field only appears if you added a member interface to cluster control link Port-Channel 48.

b) In the **Cluster Key** field, configure an authentication key for control traffic on the cluster control link.

   The shared secret is an ASCII string from 1 to 63 characters. The shared secret is used to generate the key. This option does not affect datapath traffic, including connection state update and forwarded packets, which are always sent in the clear.

c) Set the **Cluster Group Name**, which is the cluster group name in the logical device configuration.

   The name must be an ASCII string from 1 to 38 characters.

d) Choose the **Management Interface**.

   This interface is used to manage the logical device. This interface is separate from the chassis management port.

e) Choose the **Address Type** for the management interface.

This information is used to configure a management interface in the ASA configuration. Set the following information:

- **Management IP Pool**—Configure a pool of Local IP addresses, one of which will be assigned to each cluster unit for the interface, by entering the starting and ending addresses separated by a hyphen.

  Include at least as many addresses as there are units in the cluster. Note that for the Firepower 9300, you must include 3 addresses per chassis, even if you do not have all module slots filled. If you plan to expand the cluster, include additional addresses. The Virtual IP address (known as the Main cluster IP address) that belongs to the current control unit is *not* a part of this pool; be sure to reserve an IP address on the same network for the Main cluster IP address. You can use IPv4 and/or IPv6 addresses.

- **Network Mask** or **Prefix Length**
- **Network Gateway**
- **Virtual IP address**—Set the management IP address of the current control unit. This IP address must be on the same network as the cluster pool addresses, but not be part of the pool.

Step 7 On the **Settings** page, complte the following.

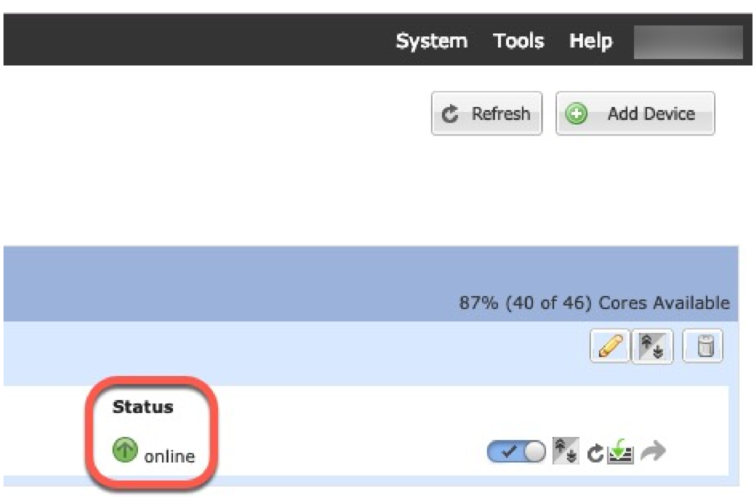
a) Enter and confirm a **Password** for the admin user.

The pre-configured ASA admin user is useful for password recovery; if you have FXOS access, you can reset the admin user password if you forget it.

Step 8 Click **OK** to close the configuration dialog box.

Step 9 Click **Save**.

The chassis deploys the logical device by downloading the specified software version and pushing the bootstrap configuration and management interface settings to the application instance. Check the **Logical Devices** page for the status of the new logical device. When the logical device shows its **Status** as **online**, you can add the remaining cluster chassis, or for intra-chassis clusteringstart configuring the cluster in the application. You may see the "Security module not responding" status as part of the process; this status is normal and is temporary.



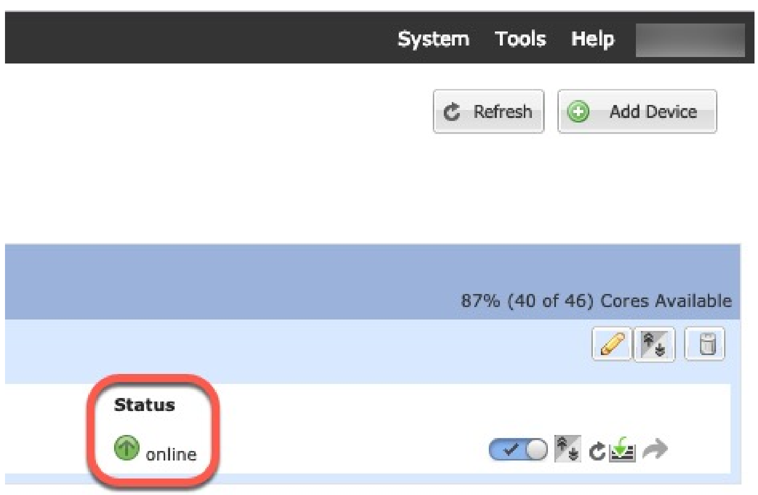
Step 10 For inter-chassis clustering, add the next chassis to the cluster:

a) On the first chassis Firepower Chassis Manager, click the **Show Configuration icon** at the top right; copy the displayed cluster configuration.
b) Connect to the Firepower Chassis Manager on the next chassis, and add a logical device according to this procedure.
c) Choose **Join an Existing Cluster**.
d) lick **OK**.
e) In the **Copy Cluster Details** box, paste in the cluster configuration from the first chassis, and click **OK**.
f) Click the device icon in the center of the screen. The cluster information is mostly pre-filled, but you must change the following settings:

   - **Chassis ID**—Enter a unique chassis ID.
   - **Cluster Key**—(Not prefilled) Enter the same cluster key.

   Click **OK**.
g) Click **Save**.

   The chassis deploys the logical device by downloading the specified software version and pushing the bootstrap configuration and management interface settings to the application instance. Check the **Logical Devices** page for each cluster member for the status of the new logical device. When the logical device for each cluster member shows its **Status** as **online**, you can start configuring the cluster in the application. You may see the "Security module not responding" status as part of the process; this status is normal and is temporary.



Step 11 Connect to the control unit ASA to customize your clustering configuration.

Add More Cluster Members

Add or replace an ASA cluster member.

> **Note** This procedure only applies to adding or replacing a *chassis*; if you are adding or replacing a module to a Firepower 9300 where clustering is already enabled, the module will be added automatically.

Before you begin

- Make sure your existing cluster has enough IP addresses in the management IP address pool for this new member. If not, you need to edit the existing cluster bootstrap configuration on each chassis before you add this new member. This change causes a restart of the logical device.
- The interface configuration must be the same on the new chassis. You can export and import FXOS chassis configuration to make this process easier.
- For multiple context mode, enable multiple context mode in the ASA application on the first cluster member; additional cluster members will inherit the multiple context mode configuration automatically.

Procedure

Step 1 On an existing cluster chassis Firepower Chassis Manager, choose **Logical Devices** to open the **Logical Devices** page.

Step 2 Click the Show Configuration icon ( ) at the top right; copy the displayed cluster configuration.

Step 3 Connect to the Firepower Chassis Manager on the new chassis, and click .

Step 4 For the **Device Name**, provide a name for the logical device.

Step 5 For the **Template**, choose **Cisco Adaptive Security Appliance**.

Step 6 For the **Image Version**, choose the ASA software version.

Step 7 For the **Device Mode**, click the **Cluster** radio button.

Step 8 Choose **Join an Existing Cluster**.

Step 9 lick **OK**.

Step 10 In the **Copy Cluster Details** box, paste in the cluster configuration from the first chassis, and click **OK**.

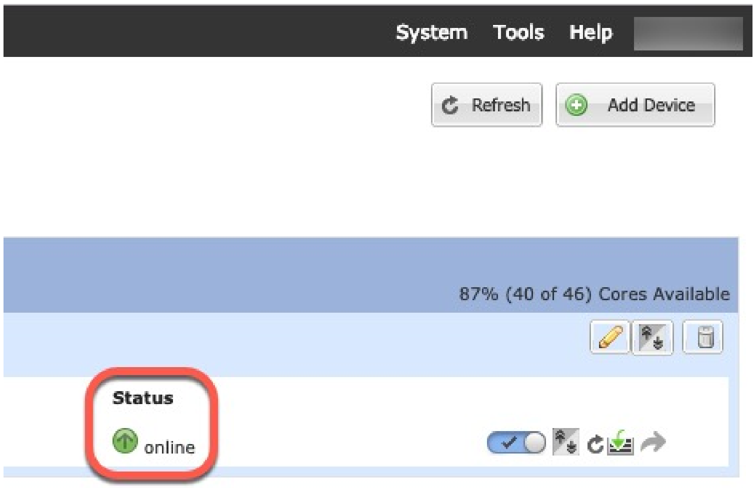
Step 11 Click the device icon in the center of the screen. The cluster information is mostly pre-filled, but you must change the following settings:

- **Chassis ID**—Enter a unique chassis ID.
- **Cluster Key**—(Not prefilled) Enter the same cluster key.

Click **OK**.

Step 12 Click **Save**.

The chassis deploys the logical device by downloading the specified software version and pushing the bootstrap configuration and management interface settings to the application instance. Check the **Logical Devices** page for each cluster member for the status of the new logical device. When the logical device for each cluster member shows its **Status** as **online**, you can start configuring the cluster in the application. You may see the "Security module not responding" status as part of the process; this status is normal and is temporary.



Manage Logical Devices

You can delete a logical device, convert an ASA to transparent mode, change the interface configuration, and perform other tasks on existing logical devices.

Connect to the Console of the Application

Use the following procedure to connect to the console of the application.

Procedure

Step 1 Connect to the module CLI.

connect module *slot_number* **console**

To connect to the security engine of a device that does not support multiple security modules, always use **1** as the *slot_number*.

Example:

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

Step 2 Connect to the application console.

Step 3 Exit the application console to the FXOS module CLI.

Step 4 Return to the supervisor level of the FXOS CLI.

a) Enter **~**

You exit to the Telnet application.

b) To exit the Telnet application, enter:

telnet>**quit**

Delete a Logical Device

Procedure

Step 1 Choose **Logical Devices** to open the Logical Devices page.

The Logical Devices page shows a list of configured logical devices on the chassis. If no logical devices have been configured, a message stating so is shown instead.

Step 2 Click **Delete** for the logical device that you want to delete.

Step 3 Click **Yes** to confirm that you want to delete the logical device.

Step 4 Click **Yes** to confirm that you want to delete the application configuration.

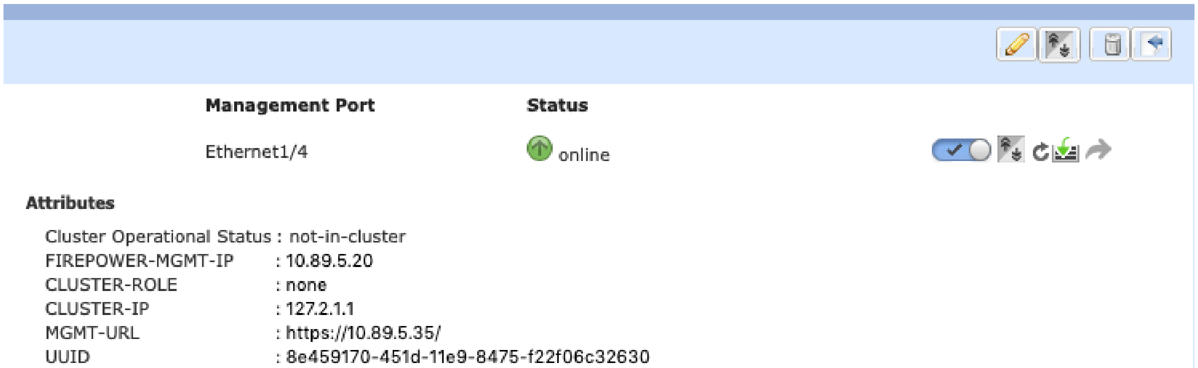
Remove a Cluster Unit

The following sections describe how to remove units temporarily or permanently from the cluster.

Temporary Removal

A cluster unit will be automatically removed from the cluster due to a hardware or network failure, for example. This removal is temporary until the conditions are rectified, and it can rejoin the cluster. You can also manually disable clustering.

To check whether a device is currently in the cluster, check the cluster status on the Firepower Chassis Manager **Logical Devices** page:



- Disable clustering in the application—You can disable clustering using the application CLI. Enter the **cluster remove unit** *name* command to remove any unit other than the one you are logged into. The bootstrap configuration remains intact, as well as the last configuration synced from the control unit, so you can later re-add the unit without losing your configuration. If you enter this command on a data unit to remove the control unit, a new control unit is elected.

  When a device becomes inactive, all data interfaces are shut down; only the Management interface can send and receive traffic. To resume traffic flow, re-enable clustering. The Management interface remains up using the IP address the unit received from the bootstrap configuration. However if you reload, and the unit is still inactive in the cluster , the Management interface is disabled.

- Disable the application instance—In Firepower Chassis Manager on the **Logical Devices** page, click the **Slider enabled** ( ). You can later reenable it using the **Slider disabled** ( ).

- Shut down the security module/engine—In Firepower Chassis Manager on the **Security Module/Engine** page, click the **Power Off icon**.

- Shut down the chassis—In Firepower Chassis Manager on the **Overview** page, click the **Shut Down icon**.

Permanent Removal

You can permanently remove a cluster member using the following methods.

- Delete the logical device—In Firepower Chassis Manager on the **Logical Devices** page, click the **Delete** ( ). You can then deploy a standalone logical device, a new cluster, or even add a new logical device to the same cluster.

- Remove the chassis or security module from service—If you remove a device from service, you can add replacement hardware as a new member of the cluster.

Change the ASA to Transparent Firewall Mode

You can only deploy a routed firewall mode ASA from the Firepower 9300 chassis. To change the ASA to transparent firewall mode, complete the initial deployment, and then change the firewall mode within the ASA CLI. For standalone ASAs, because changing the firewall mode erases the configuration, you must then redeploy the configuration from the Firepower 9300 chassis to regain the bootstrap configuration. The ASA then remains in transparent mode with a working bootstrap configuration. For clustered ASAs, the configuration is not erased, so you do not need to redeploy the bootstrap configuration from FXOS.

Procedure

Step 1 Connect to the ASA console according to Connect to the Console of the Application, on page 109. For a cluster, connect to the primary unit. For a failover pair, connect to the active unit.

Step 2 Enter configuration mode:

enable

configure terminal

By default, the enable password is blank.

Step 3 Set the firewall mode to transparent:

firewall transparent

Step 4 Save the configuration:

write memory

For a cluster or failover pair, this configuration is replicated to secondary units:

```
asa(config)# firewall transparent
asa(config)# write memory
Building configuration...
Cryptochecksum: 9f831dfb 60dffa8c 1d939884 74735b69

3791 bytes copied in 0.160 secs
[OK]
asa(config)#
Beginning configuration replication to unit-1-2
 End Configuration Replication to data unit.

asa(config)#
```

Step 5 On the Firepower Chassis Manager **Logical Devices** page, click the **Edit** icon to edit the ASA.

The **Provisioning** page appears.

Step 6 Click the device icon to edit the bootstrap configuration. Change any value in your configuration, and click **OK**.

You must change the value of at least one field, for example, the **Password** field.

You see a warning about changing the bootstrap configuration; click **Yes**.

Step 7 For an inter-chassis cluster or for a failover pair, repeat steps 5 through 7 to redeploy the bootstrap configuration on each chassis.

Wait several minutes for the chassis/security modules to reload, and for the ASA to become operational again. The ASA now has an operational bootstrap configuration, but remains in transparent mode.

Change an Interface on a Firepower Threat Defense Logical Device

You can allocate or unallocate an interface, or replace a management interface on the FTD logical device. You can then sync the interface configuration in .

Adding a new interface, or deleting an unused interface has minimal impact on the FTD configuration. However, deleting an interface that is used in your security policy will impact the configuration. Interfaces can be referenced directly in many places in the FTD configuration, including access rules, NAT, SSL, identity rules, VPN, DHCP server, and so on. Policies that refer to security zones are not affected. You can also edit the membership of an allocated EtherChannel without affecting the logical device or requiring a sync on the .

Before you begin

- Configure your interfaces, and add any EtherChannels according to Configure a Physical Interface, on page 83 and Add an EtherChannel (Port Channel), on page 84.
- If you want to add an already-allocated interface to an EtherChannel (for example, all interfaces are allocated by default to a cluster), you need to unallocate the interface from the logical device first, then add the interface to the EtherChannel. For a new EtherChannel, you can then allocate the EtherChannel to the device.
- If you want to replace the management or firepower eventing interface with a management EtherChannel, then you need to create the EtherChannel with at least 1 unallocated data member interface, and then replace the current management interface with the EtherChannel. After the FTD reboots (management interface changes cause a reboot), and you sync the configuration in , you can add the (now unallocated) management interface to the EtherChannel as well.
- For clustering or High Availability, make sure you add or remove the interface on all units before you sync the configuration in the . We recommend that you make the interface changes on the data/standby unit(s) first, and then on the control/active unit. Note that new interfaces are added in an administratively down state, so they do not affect interface monitoring.

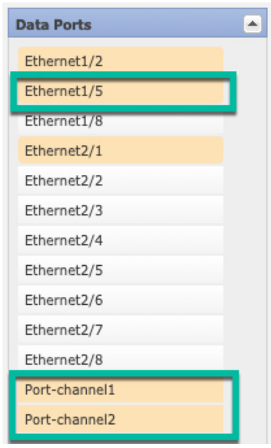
Procedure

Step 1 In the Firepower Chassis Manager, choose **Logical Devices**.

Step 2 Click the **Edit** icon at the top right to edit the logical device.

Step 3 Allocate a new data interface by selecting the interface in the **Data Ports** area.

Do not delete any interfaces yet.



Step 4 Replace the management or eventing interface:

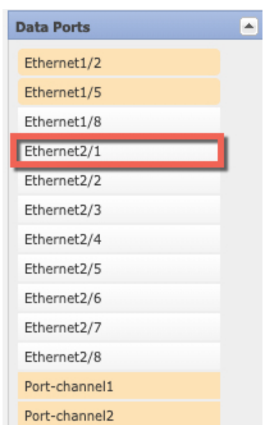
For these types of interfaces, the device reboots after you save your changes.

a) Click the device icon in the center of the page.
b) On the **General** or **Cluster Information** tab, choose the new **Management Interface** from the drop-down list.
c) On the **Settings** tab, choose the new **Eventing Interface** from the drop-down list.
d) Click **OK**.

If you change the IP address of the Management interface, then you must also change the IP address for the device in the Firepower Management Center: go to **Devices** > **Device Management** > **Device/Cluster**. In the **Management** area, set the IP address to match the bootstrap configuration address.

Step 5 Click **Save**.

Step 6 In Firepower Chassis Manager, unallocate a data interface by de-selecting the interface in the **Data Ports** area.



Step 7 Click **Save**.

Step 8 Sync the interfaces again in .

Change an Interface on an ASA Logical Device

You can allocate, unallocate, or replace a management interface on an ASA logical device. ASDM discovers the new interfaces automatically.

Adding a new interface, or deleting an unused interface has minimal impact on the ASA configuration. However, if you remove an allocated interface in FXOS (for example, if you remove a network module, remove an EtherChannel, or reassign an allocated interface to an EtherChannel), and the interface is used in your security policy, removal will impact the ASA configuration. In this case, the ASA configuration retains the original commands so that you can make any necessary adjustments. You can manually remove the old interface configuration in the ASA OS.

Note You can edit the membership of an allocated EtherChannel without impacting the logical device.

Before you begin

- Configure your interfaces and add any EtherChannels according to Configure a Physical Interface, on page 83 and Add an EtherChannel (Port Channel), on page 84.
- If you want to add an already-allocated interface to an EtherChannel (for example, all interfaces are allocated by default to a cluster), you need to unallocate the interface from the logical device first, then add the interface to the EtherChannel. For a new EtherChannel, you can then allocate the EtherChannel to the device.
- If you want to replace the management interface with a management EtherChannel, then you need to create the EtherChannel with at least 1 unallocated data member interface, and then replace the current management interface with the EtherChannel. After the ASA reloads (management interface changes cause a reload), you can add the (now unallocated) management interface to the EtherChannel as well.
- For clustering or failover, make sure you add or remove the interface on all units. We recommend that you make the interface changes on the data/standby unit(s) first, and then on the control/active unit. New interfaces are added in an administratively down state, so they do not affect interface monitoring.

Procedure

Step 1 In the Firepower Chassis Manager, choose **Logical Devices**.

Step 2 Click the **Edit** icon at the top right to edit the logical device.

Step 3 Unallocate a data interface by de-selecting the interface in the **Data Ports** area.

Step 4 Allocate a new data interface by selecting the interface in the **Data Ports** area.

Step 5 Replace the management interface:

For this type of interface, the device reloads after you save your changes.

a) Click the device icon in the center of the page.
b) On the **General/Cluster Information** tab, choose the new **Management Interface** from the drop-down list.
c) Click **OK**.

Step 6 Click **Save**.

Modify or Recover Bootstrap Settings for a Logical Device

You can modify bootstrap settings for a logical device. You can then immediately restart the application instance using those new settings or save the changes and restart the application instance using those new settings at a later time.

Procedure

Step 1 In the Firepower Chassis Manager, choose **Logical Devices**.

Step 2 Click the **Edit** icon at the top right to edit the logical device.

Step 3 Click the device icon in the center of the page.

Step 4 Modify the logical device settings as required.

Step 5 Click **OK**.

Step 6 Click **Save** to save the changes and restart the application instance.

Logical Devices Page

Use the **Logical Devices** page of the Firepower Chassis Manager to create, edit, and delete logical devices. The **Logical Devices** page includes an informational area for the logical device(s) installed on each Firepower 9300 chassis security module/engine.

The header for each logical device area provides the following information:

- The unique name of the logical device.
- The logical device mode, either Standalone or Clustered.
- **Status**—Shows the state of the logical device:
  - ok—The logical device configuration is complete.
  - incomplete-configuration—The logical device configuration is incomplete.

Each logical device area provides the following information:

- **Security Module**—Shows the security module.
- **Ports**—Shows the ports assigned to the application instance.
- **Application**—Shows the application running on the security module.
- **Version**—Shows the software version number of the application running on the security module.
- **Management IP**—Shows the local IP address assigned as the logical device Management IP.
- **Management URL**—Shows the management URL assigned to the application instance.

- **Gateway**—Shows the network gateway address assigned to the application instance.
- **Management Port**—Shows the management port assigned to the application instance.
- **Status**—Shows the state of the application instance:
  - Online—The application is running and operating.
  - Offline—The application is stopped and inoperable.
  - Installing—The application installation is in progress.
  - Not Installed—The application is not installed.
  - Install Failed—The application installation failed.
  - Starting—The application is starting up.
  - Start Failed—The application failed to start up.
  - Started—The application started successfully, and is waiting for app agent heartbeat.
  - Stopping—The application is in the process of stopping.
  - Stop Failed—The application was unable to be brought offline.
  - Not Responding—The application is unresponsive.
  - Updating—The application software update is in progress.
  - Update Failed—The application software update failed.
  - Update Succeeded—The application software update succeeded.
  - Unsupported—The installed application is not supported.
- **Attributes**—Shows additional attributes for the application instance that is currently running.

  Note If you modify the bootstrap settings for an application without immediately restarting the application instance, the Attributes fields show information for the application that is currently running and will not reflect the changes that were made until the application is restarted.

  - **Cluster Operation Status**—Shows the management URL assigned to the application instance.
  - **Management IP/Firepower Management IP**—Shows the management IP address assigned to the application instance.
  - **Cluster Role**—Shows the cluster role for the application instance, control or data.
  - **Cluster IP**—Shows the IP address assigned to the application instance.
  - **HA Role**—Shows the high-availability role for the application instance, active or standby.
  - **Management URL**—Shows the URL of the management application assigned to the application instance.
  - **UUID**—Shows the universally unique identifier for the application instance.

From the **Logical Devices** page of the Firepower Chassis Manager, you can perform the following functions on a logical device:

- **Add Device**—Allows you to create a logical device.
- **Edit**—Allows you to edit an existing logical device.
- **Update Version**—Allows you to upgrade or downgrade the software on a logical device.
- **Delete**—Deletes a logical device.
- **Show Configuration**—Opens a dialog box showing the configuration information in JSON format for a logical device or cluster. You can copy the configuration information and use it when creating additional devices that are part of a cluster.
- **Enable/Disable**—Enables or disables an application instance.
- **Go To Device Manager**—Provides a link to the Firepower Management Center or ASDM defined for the application instance.

Examples for Inter-Site Clustering

The following examples show supported cluster deployments.

Spanned EtherChannel Routed Mode Example with Site-Specific MAC Addresses

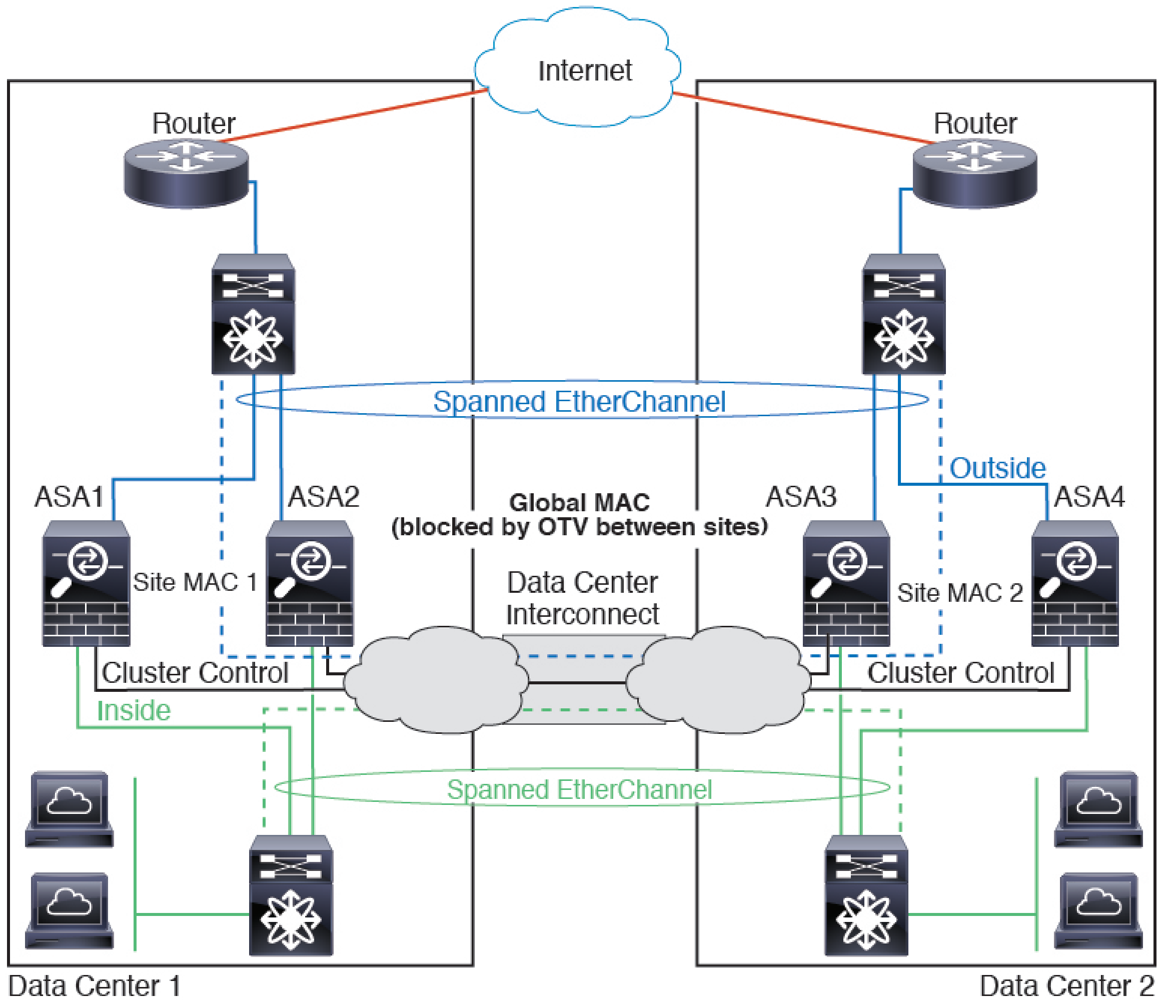
The following example shows 2 cluster members at each of 2 data centers placed between the gateway router and an inside network at each site (East-West insertion). The cluster members are connected by the cluster control link over the DCI. The cluster members at each site connect to the local switches using spanned EtherChannels for both the inside and outside networks. Each EtherChannel is spanned across all chassis in the cluster.

The data VLANs are extended between the sites using Overlay Transport Virtualization (OTV) (or something similar). You must add filters blocking the global MAC address to prevent traffic from traversing the DCI to the other site when the traffic is destined for the cluster. If the cluster units at one site become unreachable, you must remove the filters so traffic can be sent to the other site’s cluster units. You should use VACLs to filter the global MAC address.Be sure to disable ARP inspection.

The cluster acts as the gateway for the inside networks. The global virtual MAC, which is shared across all cluster units, is used only to receive packets. Outgoing packets use a site-specific MAC address from each DC cluster. This feature prevents the switches from learning the same global MAC address from both sites on two different ports, which causes MAC flapping; instead, they only learn the site MAC address.

In this scenario:

- All egress packets sent from the cluster use the site MAC address and are localized at the data center.
- All ingress packets to the cluster are sent using the global MAC address, so they can be received by any of the units at both sites; filters at the OTV localize the traffic within the data center.



Spanned EtherChannel Transparent Mode North-South Inter-Site Example

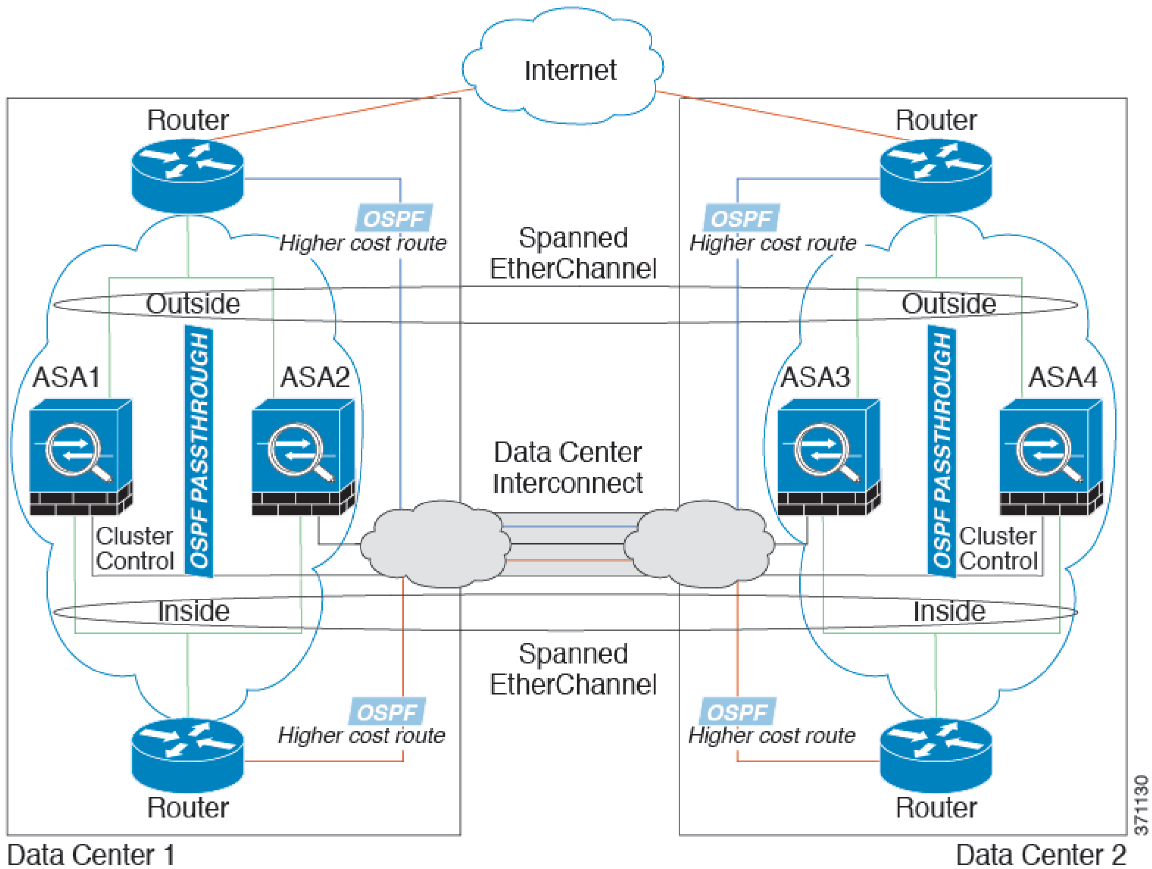
The following example shows 2 cluster members at each of 2 data centers placed between inside and outside routers (North-South insertion). The cluster members are connected by the cluster control link over the DCI. The cluster members at each site connect to the local switches using spanned EtherChannels for the inside and outside. Each EtherChannel is spanned across all chassis in the cluster.

The inside and outside routers at each data center use OSPF, which is passed through the transparent ASAs. Unlike MACs, router IPs are unique on all routers. By assigning a higher cost route across the DCI, traffic stays within each data center unless all cluster members at a given site go down. The lower cost route through the ASAs must traverse the same bridge group at each site for the cluster to maintain asymmetric connections. In the event of a failure of all cluster members at one site, traffic goes from each router over the DCI to the cluster members at the other site.

The implementation of the switches at each site can include:

- Inter-site VSS/vPC—In this scenario, you install one switch at Data Center 1, and the other at Data Center 2. One option is for the cluster units at each Data Center to only connect to the local switch, while the VSS/vPC traffic goes across the DCI. In this case, connections are for the most part kept local to each datacenter. You can optionally connect each unit to both switches across the DCI if the DCI can handle the extra traffic. In this case, traffic is distributed across the data centers, so it is essential for the DCI to be very robust.

- Local VSS/vPC at each site—For better switch redundancy, you can install 2 separate VSS/vPC pairs at each site. In this case, although the cluster units still have a spanned EtherChannel with Data Center 1 chassis connected only to both local switches, and Data Center 2 chassis connected to those local switches, the spanned EtherChannel is essentially "split." Each local VSS/vPC sees the spanned EtherChannel as a site-local EtherChannel.

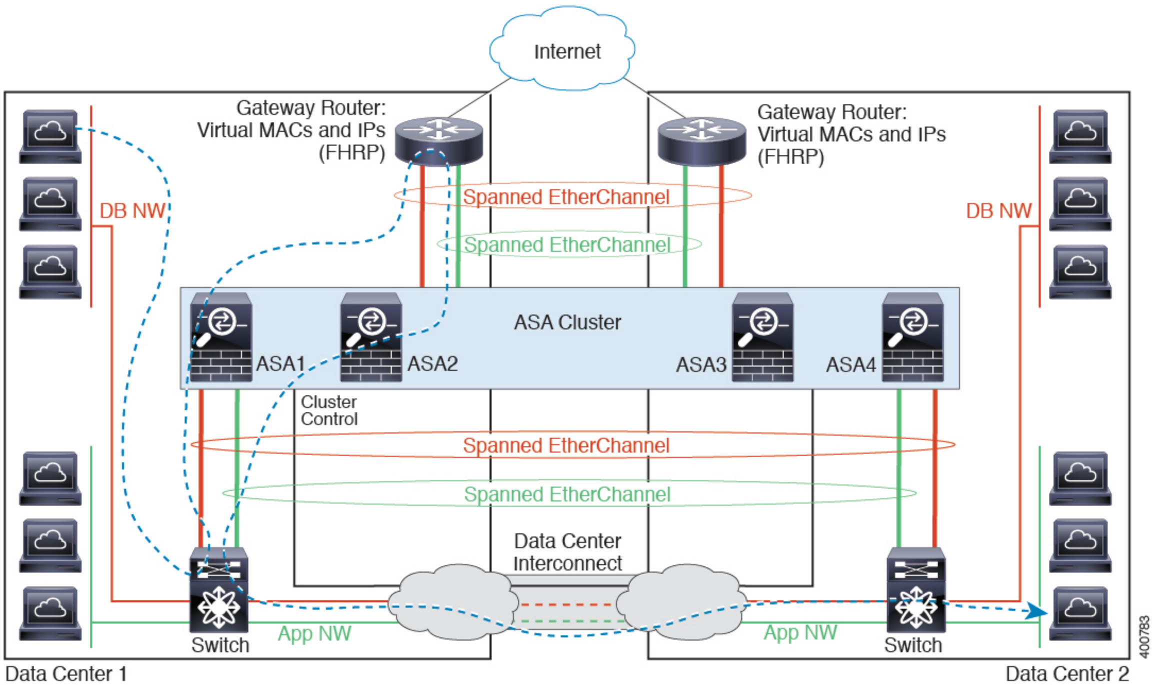


Spanned EtherChannel Transparent Mode East-West Inter-Site Example

The following example shows 2 cluster members at each of 2 data centers placed between the gateway router and two inside networks at each site, the App network and the DB network (East-West insertion). The cluster members are connected by the cluster control link over the DCI. The cluster members at each site connect to the local switches using spanned EtherChannels for both the App and DB networks on the inside and outside. Each EtherChannel is spanned across all chassis in the cluster.

The gateway router at each site uses an FHRP such as HSRP to provide the same destination virtual MAC and IP addresses at each site. A good practice to avoid unintended MAC address flapping is to statically add the gateway routers real MAC addresses to the ASA MAC address table. Without these entries, if the gateway at site 1 communicates with the gateway at site 2, that traffic might pass through the ASA and attempt to reach site 2 from the inside interface and cause problems. The data VLANs are extended between the sites using

Overlay Transport Virtualization (OTV) (or something similar). You must add filters to prevent traffic from traversing the DCI to the other site when the traffic is destined for the gateway router. If the gateway router at one site becomes unreachable, you must remove the filters so traffic can be sent to the other site's gateway router.



See Spanned EtherChannel Transparent Mode North-South Inter-Site Example, on page 119 for information about vPC/VSS options.

History for Logical Devices

Feature Name	Platform Releases	Feature Information
Inter-chassis clustering for 16 ASA modules on the Firepower 9300	1.1.3	You can now enable inter-chassis clustering for the ASA. You can include up to 16 modules. For example, you can use 1 module in 16 chassis, or 2 modules in 8 chassis, or any combination that provides a maximum of 16 modules. We modified the following screen: **Logical Devices** > **Configuration**
Intra-chassis Clustering for the ASA on the Firepower 9300	1.1.1	You can cluster all ASA security modules within the Firepower 9300 chassis. We introduced the following screen: **Logical Devices** > **Configuration**

CHAPTER 9

Security Module/Engine Management

About FXOS Security Modules/Security Engine

From the Security Modules/Security Engine page of the Firepower Chassis Manager, you can view the status of a security module/engine and can perform various functions on the security module/engine:

The Security Modules/Security Engine page provides the following information:

- Hardware State—Shows the state of the security module/engine hardware.
    - Up—The security module/engine has powered up successfully and is not showing any hardware faults, even if the security module/engine does not have a logical device associated with it.
    - Booting Up—The security module/engine is in the process of powering up.
    - Restart—The security module/engine is in the process of being restarted.
    - Down—The security module/engine is not powered on or a hardware fault is preventing the security module/engine from starting successfully.
    - Mismatch—The security module has been decommissioned or a new security module was installed into the slot. Use the Recommission or Acknowledge function to return the security module to a functioning state.
- Service State—Shows the state of the software on the security module/engine:
    - Not-available—The security module has been removed from the chassis slot. Reinstall the security module to return it to its normal operational state.
    - Online—The security module/engine is installed and is in normal operation mode.
    - Not Responding—The security module/engine is unresponsive.

- Token Mismatch—Indicates that a security module other than the one previously configured has been installed into the chassis slot. This could also be caused by a software installation error. Use the Reinitialize function to return the security module to a functioning state.
- Fault—The security module/engine is in a fault state. Review the system fault listing for more information about what might be causing the fault state.

- Power—Shows the power status of the security module/engine:
  - On—Use the Power off/on function to toggle the power status for the security module/engine.
  - Off—Use the Power off/on function to toggle the power status for the security module/engine.
- Application—Shows the logical device type that is installed on the security module/engine.

From the Security Modules/Security Engine page of the Firepower Chassis Manager, you can perform the following functions on a security module/engine:

- Decommission (security modules only)—Decommissioning a security module places the security module into maintenance mode. You can also decommission and then acknowledge a security module in order to correct certain fault states. See Decommissioning a Security Module, on page 124.
- Acknowledge—Brings newly installed security modules online. See Acknowledge a Security Module/Engine, on page 125.
- Power Cycle—Restarts the security module/engine. See Power-Cycling a Security Module/Engine, on page 125.
- Reinitialize—Reformats the security module/engine hard disk, removing all deployed applications and configurations from the security module/engine, and then restarts the system. After reinitialization is complete, if a logical device is configured for the security module/engine, the Firepower eXtensible Operating System will reinstall the application software, redeploy the logical device, and auto start the application. See Reinitializing a Security Module/Engine, on page 125.

Warning All application data on the security module/engine is deleted during reinitialization. Please back up all application data before reinitializing a security module/engine.

- Power off/on—Toggles the power state for the security module/engine. See Power-Cycling a Security Module/Engine, on page 125.

Decommissioning a Security Module

When you decommission a security module, the security module object is deleted from the configuration and the security module becomes unmanaged. Any logical devices or software running on the security module will become inactive.

You can decommission a security module if you want to temporarily discontinue use of the security module.

Procedure

Step 1 Choose **Security Modules** to open the Security Modules page.

Step 2 To decommission a security module, click **Decommission** for that security module.

Step 3 Click **Yes** to verify that you want to decommission the specified security module.

Acknowledge a Security Module/Engine

When a new security module is installed into the chassis, you must acknowledge the security module before you can begin using it.

If the security module is showing a status of “mismatch” or “token mismatch,” this is an indication that the security module installed in the slot has data on it that does not match what was previously installed in the slot. If the security module has existing data on it and you are sure you want to use it in the new slot (in other words, the security module wasn't inadvertently installed into the wrong slot), you must reinitialize the security module before you can deploy a logical device to it.

Procedure

Step 1 Choose **Security Modules/Security Engine** to open the Security Modules/Security Engine page.

Step 2 Click **Acknowledge** for the security module/engine that you want to acknowledge.

Step 3 Click **Yes** to verify that you want to acknowledge the specified security module/engine.

Power-Cycling a Security Module/Engine

Follow these steps to power-cycle a security module/engine.

Procedure

Step 1 Choose **Security Modules/Security Engine** to open the Security Modules/Security Engine page.

Step 2 Click **Power Cycle** for the security module/engine that you want to reboot.

Step 3 Click **Yes** to verify that you want to power-cycle the specified security module/engine.

Reinitializing a Security Module/Engine

When a security module/engine is reinitialized, the security module/engine hard disk is formatted and all installed application instances, configurations, and data are removed. After reinitialization has completed, if a logical device is configured for the security module/engine, FXOS will reinstall the application software, redeploy the logical device, and auto start the application.

Caution All application data on the security module/engine is deleted during reinitialization. Back up all application data before reinitializing a security module/engine.

Procedure

Step 1 Choose **Security Modules/Security Engine** to open the Security Modules/Security Engine page.

Step 2 Click **Reinitialize** for the security module/engine that you want to reinitialize.

Step 3 Click **Yes** to verify that you want to reinitialize the specified security module/engine.

The security module/engine is restarted and all data on the security module is deleted. This process can take several minutes.

CHAPTER 10

Configuration Import/Export

About Configuration Import/Export

You can use the configuration export feature to export an XML file containing logical device and platform configuration settings for your Firepower 9300 chassis to a remote server or your local computer. You can later import that configuration file to quickly apply the configuration settings to your Firepower 9300 chassis to return to a known good configuration or to recover from a system failure.

Guidelines and Restrictions

- Do not modify the contents of the configuration file. If a configuration file is modified, configuration import using that file might fail.
- Application-specific configuration settings are not contained in the configuration file. You must use the configuration backup tools provided by the application to manage application-specific settings and configurations.
- When you import a configuration to the Firepower 9300 chassis, all existing configuration on the Firepower 9300 chassis (including any logical devices) are deleted and completely replaced by the configuration contained in the import file.
- Except in an RMA scenario, we recommend you only import a configuration file to the same Firepower 9300 chassis where the configuration was exported.
- The platform software version of the Firepower 9300 chassis where you are importing should be the same version as when the export was taken. If not, the import operation is not guaranteed to be successful. We recommend you export a backup configuration whenever the Firepower 9300 chassis is upgraded or downgraded.
- The Firepower 9300 chassis where you are importing must have the same Network Modules installed in the same slots as when the export was taken.
- The Firepower 9300 chassis where you are importing must have the correct software application images installed for any logical devices defined in the export file that you are importing.

- To avoid overwriting existing backup files, change the file name in the backup operation or copy the existing file to another location.

Exporting an FXOS Configuration File

Use the configuration export feature to export an XML file containing logical device and platform configuration settings for your Firepower 9300 chassis to a remote server or your local computer.

Before you begin

Review the About Configuration Import/Export.

Procedure

Step 1 Choose **System** > **Configuration** > **Export**.

Step 2 To export a configuration file to your local computer:

a) Click **Local**.
b) Click **Export**.
The configuration file is created and, depending on your browser, the file might be automatically downloaded to your default download location or you might be prompted to save the file.

Step 3 To export the configuration file to a remote server:

a) Click **Remote**.
b) Choose the protocol to use when communicating with the remote server. This can be one of the following: FTP, TFTP, SCP, or SFTP.
c) Enter the hostname or IP address of the location where the backup file should be stored. This can be a server, storage array, local drive, or any read/write media that the Firepower 9300 chassis can access through the network.

If you use a hostname rather than an IP address, you must configure a DNS server.

d) If you are using a non-default port, enter the port number in the **Port** field.
e) Enter the username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP.
f) Enter the password for the remote server username. This field does not apply if the protocol is TFTP.
g) In the **Location** field, enter the full path to where you want the configuration file exported including the filename.
h) Click **Export**.
The configuration file is created and exported to the specified location.

Importing a Configuration File

You can use the configuration import feature to apply configuration settings that were previously exported from your Firepower 9300 chassis. This feature allows you to return to a known good configuration or to recover from a system failure.

Before you begin

Review the About Configuration Import/Export.

Procedure

Step 1 Choose **System** > **Tools** > **Import/Export**.

Step 2 To import from a local configuration file:

a) Click **Local**.
b) Click **Choose File** to navigate to and select the configuration file that you want to import.
c) Click **Import**.
A confirmation dialog box opens asking you to confirm that you want to proceed and warning you that the chassis might need to restart.
d) Click **Yes** to confirm that you want to import the specified configuration file.
The existing configuration is deleted and the configuration specified in the import file is applied to the Firepower 9300 chassis. If there is a breakout port configuration change during the import, the Firepower 9300 chassis will need to restart.

Step 3 To import from a configuration file on a remote server:

a) Click **Remote**.
b) Choose the protocol to use when communicating with the remote server. This can be one of the following: FTP, TFTP, SCP, or SFTP.
c) If you are using a non-default port, enter the port number in the **Port** field.
d) Enter the hostname or IP address of the location where the backup file is stored. This can be a server, storage array, local drive, or any read/write media that the Firepower 9300 chassis can access through the network.

If you use a hostname rather than an IP address, you must configure a DNS server.

e) Enter the username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP.
f) Enter the password for the remote server username. This field does not apply if the protocol is TFTP.
g) In the **File Path** field, enter the full path to the configuration file including the file name.
h) Click **Import**.
A confirmation dialog box opens asking you to confirm that you want to proceed and warning you that the chassis might need to restart.
i) Click **Yes** to confirm that you want to import the specified configuration file.
The existing configuration is deleted and the configuration specified in the import file is applied to the Firepower 9300 chassis. If there is a breakout port configuration change during the import, the Firepower 9300 chassis will need to restart.

CHAPTER 11

Packet Capture

Packet Capture

The Packet Capture tool is a valuable asset for use in debugging connectivity and configuration issues and for understanding traffic flows through your Firepower 9300 chassis. You can use the Packet Capture tool to log traffic that is going through specific interfaces on your Firepower 9300 chassis.

You can create multiple packet capture sessions, and each session can capture traffic on multiple interfaces. For each interface included in a packet capture session, a separate packet capture (PCAP) file will be created.

Backplane Port Mappings

The Firepower 9300 chassis uses the following mappings for internal backplane ports:

Security Module	Port Mapping	Description
Security Module 1/Security Engine	Ethernet1/9	Internal-Data0/0
Security Module 1/Security Engine	Ethernet1/10	Internal-Data0/1
Security Module 2	Ethernet1/11	Internal-Data0/0
Security Module 2	Ethernet1/12	Internal-Data0/1
Security Module 3	Ethernet1/13	Internal-Data0/0
Security Module 3	Ethernet1/14	Internal-Data0/1

Guidelines and Limitations for Packet Capture

The Packet Capture tool has the following limitations:

- Can capture only up to 100 Mbps.
- Packet capture sessions can be created even when there is not enough storage space available to run the packet capture session. You should verify that you have enough storage space available before you start a packet capture session.
- Does not support multiple active packet capturing sessions.
- There is no option to filter based on source or destination IPv6 address.
- Captures only at the ingress stage of the internal switch.
- Filters are not effective on packets that cannot be understood by the internal switch (for example Security Group Tag and Network Service Header packets).
- You cannot capture packets for an EtherChannel as a whole. However, for an EtherChannel allocated to a logical device, you can capture packets on each member interface of the EtherChannel.
- You cannot copy or export a PCAP file while the capture session is still active.
- When you delete a packet capture session, all packet capture files associated with that session are also deleted.

Creating or Editing a Packet Capture Session

Procedure

Step 1 Choose **Tools** > **Packet Capture**.

The **Capture Session** tab displays a list of currently configured packet capture sessions. If no packet capture sessions are currently configured, a message stating so is displayed instead.

Step 2 Do one of the following:

- To create a packet capture session, click the **Capture Session** button.
- To edit an existing packet capture session, click the **Edit** button for that session.

The left side of the window lets you select a specific application instance and then shows a representation of that instance. This representation is used to select the interfaces on which you would like to capture packets. The right side of the window contains fields for defining the packet capture session.

Step 3 On the left side of the window, click the name of the application instance for which you would like to capture packets.

Step 4 Click the interfaces on which you want to capture traffic. Selected interfaces show a check mark.

Step 5 To capture traffic from the logical device going out over the backplane ports:

a) Click the box representing the application instance.

The **Capture On**, **Application Port**, and **Application Capture Direction** fields are made available on the right side of the **Configure Packet Capture Session** window.

b) Select the backplane port you wish to capture traffic on or select **All Backplane Ports** from the **Capture On** drop-down list.

Step 6 Enter a name for the packet capture session in the **Session Name** field.

Step 7 Specify the buffer size to use for this packet capture session by selecting one of the pre-defined values from the **Buffer Size** list, or by selecting **Custom in MB** and then entering the desired buffer size. The specified buffer size must be between 256 and 2048 MB.

Step 8 Specify whether you want to overwrite existing PCAP files or append data to the PCAP files when this packet capture session is executed.

Step 9 To capture traffic between the application instance and a specific interface:

a) Click the box representing the logical device.
b) From the **Capture On** drop-down list, choose the application type (for example, **asa**).
c) Select the **Application Port** that you would like to capture traffic coming from or going to.
d) To capture only the traffic going from the logical device toward the specified interface, click the **Egress Packets** option next to **Application Capture Direction**.

Note If you choose **Egress Packets**, traffic will be captured only on the selected backplane ports—traffic will not be captured on physical ports even if you have selected them.

e) To capture traffic coming from or going to the specified interface, click the **All Packets** option next to **Application Capture Direction**.

Step 10 To filter the traffic being captured:

a) Click the **Apply Filter** option for the **Capture Filter** field.

You are given a set of fields for configuring the filter.

b) If you need to create the filter, click **Create Filter**.

You see the **Create Packet Filter** dialog box. For more information, see Configuring Filters for Packet Capture, on page 134.

c) Select the filter you want to use from the **Apply** drop-down list.
d) Select the interface to which you want to apply the filter from the **To** drop-down list.
e) To apply additional filters, click **Apply Another Filter** and then repeat the steps above to apply the additional filter.

Step 11 Do one of the following:

- To save this packet capture session and run it now, click the **Save and Run** button. This option is only available if no other packet capture sessions are currently running.
- To save this packet capture session so that it can be ran at a later time, click the **Save** button.

You see the **Capture Session** tab with your session listed along with any other sessions that have been created. If you selected **Save and Run**, your packet capture session will be capturing packets. You will need to stop capturing before you can download the PCAP files from your session.

Configuring Filters for Packet Capture

You can create filters to limit the traffic that is included in a packet capture session. You can select which interfaces should use a specific filter while creating a packet capture session.

Note If you modify or delete a filter that is applied to a packet capture session that is currently running, the changes will not take affect until you disable that session and then reenable it.

Procedure

Step 1 Choose **Tools** > **Packet Capture**.

The **Capture Session** tab displays a list of currently configured packet capture sessions. If no packet capture sessions are currently configured, a message stating so is displayed instead.

Step 2 Do one of the following:

- To create a filter, click the **Add Filter** button.
- To edit an existing filter, click the **Edit** button for that fitler.

You see the **Create or Edit Packet Filter** dialog box.

Step 3 Enter a name for the packet capture filter in the **Filter Name** field.

Step 4 To filter on a specific protocol, select it from the **Protocol** list, or select**Custom** and then enter the desired protocol. The custom protocol must be an IANA defined protocol in decimal format (0-255).

Step 5 To filter on a specific EtherType, select it from the **EtherType** list, or select**Custom** and then enter the desired EtherType. The custom EhterType must be an IANA defined EtherType in decimal format (for example, IPv4 = 2048, IPv6 = 34525, ARP = 2054, and SGT = 35081).

Step 6 To filter traffic based on an Inner VLAN (VLAN ID while ingressing the port) or Outer VLAN (VLAN ID added by the Firepower 9300 chassis), enter the VLAN ID in the specified field.

Step 7 To filter traffic from a specific source or destination, enter the IP address and port or enter the MAC address in the specified source or destination fields.

Step 8 Click **Save** to save the filter,

You see the **Filter List** tab with your filter listed along with any other filters that have been created.

Starting and Stopping a Packet Capture Session

Procedure

Step 1 Choose **Tools** > **Packet Capture**.

The **Capture Session** tab displays a list of currently configured packet capture sessions. If no packet capture sessions are currently configured, a message stating so is displayed instead.

Step 2 To start a packet capture session, click the **Enable Session** button for that session and then click **Yes** to confirm.

Note You cannot start a packet capture session while another session is running.

The PCAP files for the interfaces included in the session will start collecting traffic. If the session is configured to overwrite session data, the existing PCAP data will be erased. If not, data will be appended to the existing file (if any).

While the packet capture session is running, the file size for the individual PCAP files will increase as traffic is captured. Once the Buffer Size limit is reached, the system will start dropping packets and you will see the Drop Count field increase.

Step 3 To stop a packet capture session, click the **Disable Session** button for that session and then click **Yes** to confirm.

After the session has been disabled, you can then download the PCAP files (see Downloading a Packet Capture File, on page 135).

Downloading a Packet Capture File

You can download the Packet Capture (PCAP) files from a session to your local computer so that they can be analyzed using a network packet analyzer.

Procedure

Step 1 Choose **Tools** > **Packet Capture**.

The **Capture Session** tab displays a list of currently configured packet capture sessions. If no packet capture sessions are currently configured, a message stating so is displayed instead.

Step 2 To download the PCAP file for a specific interface from a packet capture session, click the **Download** button that corresponds to that interface.

Note You cannot download a PCAP file while a packet capture session is running.

Depending on your browser, the specified PCAP file is either automatically downloaded to your default download location or you are prompted to save the file.

INDEX

N

P

R

S

T

U