CONTENTS

CHAPTER 1

Introduction to the Firepower Security Appliance  1
  About the Firepower Security Appliance  1
  Firepower Chassis Manager Overview  1
  Monitoring the Chassis Status  2

CHAPTER 2

Getting Started  5
  Task Flow  5
  Initial Configuration  5
  Log In or Out of the Firepower Chassis Manager  8
  Accessing the FXOS CLI  9

CHAPTER 3

License Management for the ASA  11
  About Smart Software Licensing  11
    Smart Software Licensing for the ASA  11
    Smart Software Manager and Accounts  12
    Licenses and Devices Managed per Virtual Account  12
    Evaluation License  12
    Smart Software Manager Communication  13
      Device Registration and Tokens  13
      Periodic Communication with the License Authority  13
    Out-of-Compliance State  13
      Smart Call Home Infrastructure  13
    Prerequisites for Smart Software Licensing  14
    Guidelines for Smart Software Licensing  14
    Defaults for Smart Software Licensing  14
    Configure Smart Software Licensing  14
Contents

Setting the Date and Time Manually 40

Configuring SSH 40

Configuring Telnet 42

Configuring SNMP 42
  About SNMP 43
  SNMP Notifications 43
  SNMP Security Levels and Privileges 44
  Supported Combinations of SNMP Security Models and Levels 44
  SNMPv3 Security Features 44
  SNMP Support 45
  Enabling SNMP and Configuring SNMP Properties 45
  Creating an SNMP Trap 46
  Deleting an SNMP Trap 47
  Creating an SNMPv3 User 48
  Deleting an SNMPv3 User 49

Configuring HTTPS 50
  Certificates, Key Rings, and Trusted Points 50
  Creating a Key Ring 51
  Regenerating the Default Key Ring 51
  Creating a Certificate Request for a Key Ring 52
    Creating a Certificate Request for a Key Ring with Basic Options 52
    Creating a Certificate Request for a Key Ring with Advanced Options 53
  Creating a Trusted Point 55
  Importing a Certificate into a Key Ring 56

Configuring HTTPS 58
  Changing the HTTPS Port 59
  Deleting a Key Ring 59
  Deleting a Trusted Point 60
  Disabling HTTPS 61

Configuring AAA 61
  About AAA 61
  Configuring LDAP Providers 62
    Configuring Properties for LDAP Providers 62
    Creating an LDAP Provider 63
Add a Standalone ASA 81
Add a High Availability Pair 82
Add a Cluster 83
  About Clustering on the Firepower 9300 Chassis 83
  Primary and Secondary Unit Roles 84
  Cluster Control Link 84
  Management Interface 84
Add an ASA Cluster 84
  Create an ASA Cluster 85
Manage Logical Devices 86
  Connect to the Console of the Application 86
  Change the ASA to Transparent Firewall Mode 88
  Change an Interface on a Firepower Threat Defense Logical Device 89
  Change an Interface on an ASA Logical Device 90
  Modify or Recover Bootstrap Settings for a Logical Device 91
Logical Devices Page 92
History for Logical Devices 94
Introduction to the Firepower Security Appliance

• About the Firepower Security Appliance, on page 1
• Firepower Chassis Manager Overview, on page 1
• Monitoring the Chassis Status, on page 2

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 73.
• Logical Devices—From the Logical Devices page, you can create, edit, and delete logical devices. For more information, see Logical Devices, on page 79.

• 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 37.

• 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 31.
  • 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 17.

## 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.
  • Mode—shows the operating mode for the chassis: standalone or cluster.
  • Overall status—shows the highest fault level 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.
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.

  You can click on any interface to see a graphical representation of the number of input and output bytes for that interface over the last fifteen minutes.

- **Devices**—Lists the logical devices configured in the system and provides the following details for each logical device: device name, device state, application template type, operational state, administrative state, image version, management IP address, and management URL.

- **License**—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.
Getting Started

- Task Flow, on page 5
- Initial Configuration, on page 5
- Log In or Out of the Firepower Chassis Manager, on page 8
- Accessing the FXOS CLI, on page 9

Task Flow

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

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Configure the Firepower 9300 chassis hardware (see the Cisco Firepower Security Appliance Hardware Installation Guide).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Complete the initial configuration (see Initial Configuration, on page 5).</td>
</tr>
<tr>
<td>Step 3</td>
<td>Log in to the Firepower Chassis Manager (see Log In or Out of the Firepower Chassis Manager, on page 8).</td>
</tr>
<tr>
<td>Step 4</td>
<td>Set the Date and Time (see Setting the Date and Time, on page 39).</td>
</tr>
<tr>
<td>Step 5</td>
<td>Configure a DNS server (see Configuring DNS Servers, on page 72).</td>
</tr>
<tr>
<td>Step 6</td>
<td>Register your product license (see License Management for the ASA, on page 11).</td>
</tr>
<tr>
<td>Step 7</td>
<td>Configure users (see User Management, on page 17).</td>
</tr>
<tr>
<td>Step 8</td>
<td>Perform software updates as required (see Image Management, on page 31).</td>
</tr>
<tr>
<td>Step 9</td>
<td>Configure additional platform settings (see Platform Settings, on page 37).</td>
</tr>
<tr>
<td>Step 10</td>
<td>Configure interfaces (see Interface Management, on page 73).</td>
</tr>
<tr>
<td>Step 11</td>
<td>Create logical devices (see Logical Devices, on page 79).</td>
</tr>
</tbody>
</table>

Initial Configuration

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. 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.

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

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Connect to the console port.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Power on the Firepower 9300 chassis.</td>
</tr>
<tr>
<td></td>
<td>You will see the power on self-test messages as the Firepower 9300 chassis boots.</td>
</tr>
<tr>
<td>Step 3</td>
<td>When the unconfigured system boots, a setup wizard prompts you for the following information required to configure the system:</td>
</tr>
<tr>
<td>Step 4</td>
<td>Review the setup summary and enter yes to save and apply the settings, or enter no to go through the Setup wizard again to change some of the settings.</td>
</tr>
<tr>
<td></td>
<td>If you choose to go through the Setup wizard again, the values you previously entered appear in brackets. To accept previously entered values, press Enter.</td>
</tr>
</tbody>
</table>

Example

The following example sets up a configuration using IPv4 management addresses:
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? (y/n) [y]: n
Enter the password for "admin": adminpassword%
Confirm the password for "admin": adminpassword%
Enter the system name: foo
Physical Switch Mgmt0 IP address : 192.168.10.10
Physical Switch Mgmt0 IPv4 netmask: 255.255.255.0
IPV4 address of the default gateway: 192.168.10.1
Do you want to configure IP block for ssh access? (yes/no) [y]: y
  SSH IPv4 block netmask: 0.0.0.0
Do you want to configure IP block for https access? (yes/no) [y]: y
  HTTPS IP block address: 0.0.0.0
  HTTPS IPv4 block netmask: 0.0.0.0
Configure the DNS Server IP address (yes/no) [n]: y
  DNS IP address: 20.10.20.10
Configure the default domain name? (yes/no) [n]: y
  Default domain name: domainname.com
Following configurations will be applied:
  Switch Fabric=A
  System Name=foo
  Enforced Strong Password=no
  Physical Switch Mgmt0 IPv6 Address=2001::107
  Physical Switch Mgmt0 IPv6 Prefix=64
  Default Gateway=2001::1
  IPV6 value=0
  SSH Access Configured=yes
  SSH IP Address=0.0.0.0
  SSH IP Netmask=0.0.0.0
  HTTPS Access Configured=yes
  HTTPS IP Address=0.0.0.0
  HTTPS IPv6 block netmask: 0.0.0.0
  DNS Server=20.10.20.10
  Domain Name=domainname.com
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes

The following example sets up a configuration using IPv6 management addresses:

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? (y/n) [y]: n
Enter the password for "admin": adminpassword%
Confirm the password for "admin": adminpassword%
Enter the system name: foo
Physical Switch Mgmt0 IP address : 2001::107
Physical Switch Mgmt0 IPv6 prefix: 64
IPV6 address of the default gateway: 2001::1
Do you want to configure IP block for ssh access? (yes/no) [y]: y
  SSH IPv6 block netmask: 0.0.0.0
Do you want to configure IP block for https access? (yes/no) [y]: y
  HTTPS IP block address: 0.0.0.0
  HTTPS IPv6 block netmask: 0.0.0.0
Configure the DNS Server IPv6 address? (yes/no) [n]: y
  DNS IP address: 2001::101
Configure the DNS Server IPv6 address (yes/no) [n]:
Configure the default domain name? (yes/no) [n]: y
  Default domain name: domainname.com
Following configurations will be applied:
  Switch Fabric=A
  System Name=foo
  Enforced Strong Password=no
  Physical Switch Mgmt0 IPv6 Address=2001::107
  Physical Switch Mgmt0 IPv6 Prefix=64
  Default Gateway=2001::1
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 17.

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 25.

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 26.

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 | UCSM-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 42 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.
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.

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.

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.

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.
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. 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 “SLProf” that specifies the URL for the Licensing Authority.

Configure 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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>(Optional) Configure the HTTP Proxy, on page 15.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Register the Firepower Security Appliance with the License Authority, on page 15.</td>
</tr>
</tbody>
</table>

---

### (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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose System &gt; Licensing &gt; Call Home.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The Call Home page provides fields for configuring the destination address URL for the License Authority and for configuring an HTTP proxy.</td>
</tr>
<tr>
<td>Note</td>
<td>Unless directed by Cisco TAC, you should not change the License Authority URL.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>In the Server Enable drop-down list, select on.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>Enter the proxy IP address and port in the Server URL and Server Port fields. For example, enter port 443 for an HTTPS server.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Save.</td>
</tr>
</tbody>
</table>

---

### 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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Smart Software Manager request and copy a registration token for the virtual account to which you want to add this Firepower 9300 chassis.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In Firepower Chassis Manager, choose System &gt; Licensing &gt; Smart License.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter the registration token in the Enter Product Instance Registration Token field.</td>
</tr>
</tbody>
</table>
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.

### History for Smart Software Licensing

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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** |
User Management

- User Accounts, on page 17
- Guidelines for Usernames, on page 18
- Guidelines for Passwords, on page 19
- Guidelines for Remote Authentication, on page 19
- User Roles, on page 22
- Password Profile for Locally Authenticated Users, on page 22
- Configuring User Settings, on page 23
- Configuring the Session Timeout, on page 25
- Set the Maximum Number of Login Attempts, on page 26
- Creating a Local User Account, on page 27
- Deleting a Local User Account, on page 28
- Activating or Deactivating a Local User Account, on page 28
- Clearing the Password History for a Locally Authenticated User, on page 29

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, including username and password.
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 19
- Configuring LDAP Providers, on page 62
- Configuring RADIUS Providers, on page 65
- Configuring TACACS+ Providers, on page 67

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 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).
• 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 TACAS+ 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:

<table>
<thead>
<tr>
<th>Authentication Provider</th>
<th>Custom Attribute</th>
<th>Schema Extension</th>
<th>Attribute ID Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP</td>
<td>Optional</td>
<td>You can choose to do one of the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Do not extend the LDAP schema and configure an existing, unused attribute that meets the requirements.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Extend the LDAP schema and create a custom attribute with a unique name, such as CiscoAVPair.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The Cisco LDAP implementation requires a unicode type attribute.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you choose to create the CiscoAVPair custom attribute, use the following attribute ID: 1.3.6.1.4.1.9.287247.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>A sample OID is provided in the following section.</td>
<td></td>
</tr>
<tr>
<td>RADIUS</td>
<td>Optional</td>
<td>You can choose to do one of the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Do not extend the RADIUS schema and use an existing, unused attribute that meets the requirements.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Extend the RADIUS schema and create a custom attribute with a unique name, such as cisco-avpair.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The vendor ID for the Cisco RADIUS implementation is 009 and the vendor ID for the attribute is 001.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following syntax example shows how to specify multiple user roles and locales if you choose to create the cisco-avpair attribute:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>use a comma &quot;,&quot; as the delimiter to separate multiple values.</td>
<td></td>
</tr>
</tbody>
</table>
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:

```plaintext
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
oSMSyntax: 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.

<table>
<thead>
<tr>
<th>Interval Configuration</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>No password change allowed</td>
<td>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.</td>
<td>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</td>
</tr>
</tbody>
</table>
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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Local</strong>—The user account must be defined locally on the Firepower chassis.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Radius</strong>—The user account must be defined on the RADIUS server specified for the Firepower chassis.</td>
</tr>
<tr>
<td></td>
<td>• <strong>TACACS</strong>—The user account must be defined on the TACACS+ server specified for the Firepower chassis.</td>
</tr>
<tr>
<td></td>
<td>• <strong>LDAP</strong>—The user account must be defined on the LDAP/MS-AD server specified for the Firepower chassis.</td>
</tr>
<tr>
<td></td>
<td>• <strong>None</strong>—If the user account is local to the Firepower chassis, no password is required when the user logs in remotely.</td>
</tr>
</tbody>
</table>

Remote User Settings
### Remote User Role Policy
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.

### Local User Settings

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Assign Default Role</strong> — The user is allowed to log in with a read-only user role.</td>
</tr>
<tr>
<td></td>
<td>- <strong>No-Login</strong> — The user is not allowed to log in to the system, even if the username and password are correct.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password Strength Check</strong> 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 19).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>History Count</strong> 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.</td>
</tr>
<tr>
<td></td>
<td>This value can be anywhere from 0 to 15.</td>
</tr>
<tr>
<td></td>
<td>You can set the <strong>History Count</strong> field to 0 to disable the history count and allow users to reuse previously used passwords at any time.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Change During Interval</strong> field</td>
<td>Controls when a locally authenticated user can change his or her password. This can be:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Enable</strong> — Locally authenticated users can change their passwords based on the settings for Change Interval and Change Count.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Disable</strong> — Locally authenticated users cannot change their passwords for the period of time specified for No Change Interval.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Change Interval</strong> field</td>
<td>The number of hours over which the number of password changes specified in the <strong>Change Count</strong> field are enforced.</td>
</tr>
<tr>
<td></td>
<td>This value can be anywhere from 1 to 745 hours.</td>
</tr>
<tr>
<td></td>
<td>For example, if this field is set to 48 and the <strong>Change Count</strong> field is set to 2, a locally authenticated user can make no more than 2 password changes within a 48 hour period.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Change Count</strong> field</td>
<td>The maximum number of times a locally authenticated user can change his or her password during the Change Interval.</td>
</tr>
<tr>
<td></td>
<td>This value can be anywhere from 0 to 10.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>No Change Interval field</td>
<td>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.</td>
</tr>
</tbody>
</table>

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**

1. Enter security mode:
   - Firepower-chassis # scope security
2. Enter default authorization security mode:
   - Firepower-chassis /security # scope default-auth
3. Set the idle timeout for HTTPS, SSH, and Telnet sessions:
   - Firepower-chassis /security/default-auth # set session-timeout seconds
4. (Optional) Set the idle timeout for console sessions:
   - Firepower-chassis /security/default-auth # set con-session-timeout seconds
5. (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
- 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:
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.

Procedure

Step 1  From the FXOS CLI, enter security mode:

```plaintext
scope system
scope security
```

Step 2  Set the maximum number of unsuccessful login attempts.

```plaintext
set max-login-attempts
max_login
```

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:

```plaintext
set user-account-unlock-time
unlock_time
```

Step 4  Commit the configuration:

```plaintext
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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name field</td>
<td>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 18). After you save the user, the login ID cannot be changed. You must delete the user account and create a new one.</td>
</tr>
<tr>
<td>First Name field</td>
<td>The first name of the user. This field can contain up to 32 characters.</td>
</tr>
<tr>
<td>Last Name field</td>
<td>The last name of the user. This field can contain up to 32 characters.</td>
</tr>
<tr>
<td>Email field</td>
<td>The email address for the user.</td>
</tr>
<tr>
<td>Phone Number field</td>
<td>The telephone number for the user.</td>
</tr>
<tr>
<td>Password field</td>
<td>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 19).</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>The password a second time for confirmation purposes.</td>
</tr>
<tr>
<td>Account Status</td>
<td>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.</td>
</tr>
<tr>
<td>User Role drop-down list</td>
<td>The role that represents the privileges you want to assign to the user account (see User Roles, on page 22).</td>
</tr>
</tbody>
</table>

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.
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.
- 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.

---

# 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 #
```
Clearing the Password History for a Locally Authenticated User
CHAPTER 5

Image Management

• About Image Management, on page 31
• Downloading Images from Cisco.com, on page 32
• Uploading an Image to the Firepower Security Appliance, on page 32
• Verifying the Integrity of an Image, on page 32
• Upgrading the Firepower eXtensible Operating System Platform Bundle, on page 33
• Updating the Image Version for a Logical Device, on page 33
• Firmware Upgrade, on page 34

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.

---

Note

• 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. For release 1.1.1, the only available application images are for the ASA. 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**

  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.

---

**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.
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 32) and then upload that image to the Firepower 9300 chassis (see Uploading an Image to the Firepower Security Appliance, on page 32).

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 slave unit.
2. Make the slave unit the master unit.
3. Change the startup version on the original master unit (now slave).

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 32) and then upload that image to the Firepower 9300 chassis (see Uploading an Image to the Firepower Security Appliance, on page 32).

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.
Firmware Upgrade

Use the following procedure to upgrade the firmware on your Firepower 9300 chassis.

Procedure

The software download page for the Firepower 9300 chassis is opened in the browser.

Step 2 Find and then download the appropriate firmware package from Cisco.com to a server that you can access from the Firepower 9300 chassis.

Step 3 On the Firepower 9300 chassis, enter firmware mode:
Firepower-chassis # scope firmware

Step 4 Download the FXOS firmware image to the Firepower 9300 chassis:
Firepower-chassis /firmware # 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 5 To monitor the download process:
Firepower-chassis /firmware # show download-task image_name detail

Step 6 After the download has completed, you can enter the following command to view the contents of the firmware package:
Firepower-chassis /firmware # show package image_name expand

Step 7 You can enter the following command to view the version number of the firmware package:
Firepower-chassis /firmware # show package
This version number is used in the following step when installing the firmware package.

Step 8 To install the firmware package:
a) Enter firmware-install mode:
Firepower-chassis /firmware # scope firmware-install

b) Install the firmware package:

Firepower-chassis /firmware/firmware-install # install firmware pack-version version_number

The system will verify the firmware package and will notify you that the verification process can take several minutes to complete.

c) Enter yes to proceed with the verification.

After verifying the firmware package, the system will notify you that the installation process can take several minutes to complete and that the system will reboot during the update process.

d) Enter yes to proceed with the installation. Do not power cycle the Firepower 9300 chassis during the upgrade process.

Step 9  To monitor the upgrade process:

Firepower-chassis /firmware/firmware-install # show detail

Step 10  After the installation has completed, you can enter the following commands to view the current firmware version:

Firepower-chassis /firmware/firmware-install # top

Firepower-chassis # scope chassis 1

Firepower-chassis /firmware # show sup version

---

Example

The following example upgrades the firmware to version 1.0.10:

Firepower-chassis# scope firmware
Firepower-chassis /firmware # download image
tftp://10.10.10.1/fxos-k9-fpr9k-firmware.1.0.10.SPA
Firepower-chassis /firmware # show download-task fxos-k9-fpr9k-firmware.1.0.10.SPA detail

Download task:
  File Name: fxos-k9-fpr9k-firmware.1.0.10.SPA
  Protocol: Tftp
  Server: 10.10.10.1
  Port: 0
  Userid:
  Path:
  Downloaded Image Size (KB): 2104
  Time stamp: 2015-12-04T23:51:57.846
  State: Downloading
  Transfer Rate (KB/s): 263.000000
  Current Task: unpacking image fxos-k9-fpr9k-firmware.1.0.10.SPA on primary(
  FSM=STAGE:sam:dme:FirmwareDownloaderDownload:UnpackLocal)

Firepower-chassis /firmware # show package fxos-k9-fpr9k-firmware.1.0.10.SPA expand

Package fxos-k9-fpr9k-firmware.1.0.10.SPA:
  Images:
    fxos-k9-fpr9k-fpga.1.0.5.bin
    fxos-k9-fpr9k-rommon.1.0.10.bin

Firepower-chassis /firmware # show package
Name                                      Version
-------------------------------------------- -------
fxos-k9-fpr9k-firmware.1.0.10.SPA          1.0.10

Firepower-chassis /firmware # **scope firmware-install**
Firepower-chassis /firmware/firmware-install # **install firmware pack-version 1.0.10**

Verifying FXOS firmware package 1.0.10. Verification could take several minutes.
Do you want to proceed? (yes/no):yes

FXOS SUP ROMMON: Upgrade from 1.0.10 to 1.0.10
FXOS SUP FPGA : Upgrade from 1.04 to 1.05

This operation upgrades SUP firmware on Security Platform.
Here is the checklist of things that are recommended before starting the install operation
(1) Review current critical/major faults
(2) Initiate a configuration backup

Attention:
The system will be reboot to upgrade the SUP firmware.
The upgrade operation will take several minutes to complete.
PLEASE DO NOT POWER RECYCLE DURING THE UPGRADE.
Do you want to proceed? (yes/no):yes

Upgrading FXOS SUP firmware software package version 1.0.10

command executed
Platform Settings

- Changing the Management IP Address, on page 37
- Setting the Date and Time, on page 39
- Configuring SSH, on page 40
- Configuring Telnet, on page 42
- Configuring SNMP, on page 42
- Configuring HTTPS, on page 50
- Configuring AAA, on page 61
- Configuring Syslog, on page 69
- Configuring DNS Servers, on page 72

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**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Connect to the FXOS CLI (see Accessing the FXOS CLI, on page 9).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>To configure an IPv4 management IP address:</td>
</tr>
<tr>
<td></td>
<td>a) Set the scope for fabric-interconnect a:</td>
</tr>
<tr>
<td></td>
<td>Firepower-chassis# scope fabric-interconnect a</td>
</tr>
<tr>
<td></td>
<td>b) To view the current management IP address, enter the following command:</td>
</tr>
<tr>
<td></td>
<td>Firepower-chassis /fabric-interconnect # show</td>
</tr>
<tr>
<td></td>
<td>c) Enter the following command to configure a new management IP address and gateway:</td>
</tr>
</tbody>
</table>
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

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
  ---- ------------- ------------- ---------------- ------------- ---------------
      ---------        ----------        --------------        --------------
   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
```
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.

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.

The Firepower chassis is configured with the NTP server information 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.
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 40).
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, and to enable the FXOS chassis as an 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 For the server Encryption Algorithm, check the check boxes for each allowed encryption algorithm.

Note 3des-cbc is not supported in Common Criteria. If Common Criteria mode is enabled on the FXOS chassis, you cannot use 3des-cbc as an encryption algorithm.

Step 4 For the server Key Exchange Algorithm, check the check boxes for each allowed Diffie-Hellman (DH) key exchange. The DH key exchange provides a shared secret that cannot be determined by either party alone. The key exchange is combined with a signature and the host key to provide host authentication. This key-exchange method provides explicit server authentication. For more information about using DH key-exchange methods, see RFC 4253.

Step 5 For the server Mac Algorithm, check the check boxes for each allowed integrity algorithm.

Step 6 For the server Host Key, enter the modulus size for the RSA key pairs.

The modulus value (in bits) is in multiples of 8 from 1024 to 2048. The larger the key modulus size you specify, the longer it takes to generate an RSA key pair. We recommend a value of 2048.

Step 7 For the server Volume Rekey Limit, set the amount of traffic in KB allowed over the connection before FXOS disconnects from the session.

Step 8 For the server Time Rekey Limit, set the minutes for how long an SSH session can be idle before FXOS disconnects the session.

Step 9 Click Save.

Step 10 Click the SSH Client tab to customize the FXOS chassis SSH client.

Step 11 For the Strict Host Key check, choose enable, disable, or prompt to control SSH host key checking.

- enable - The connection is rejected if the host key is not already in the FXOS known hosts file. You must manually add hosts at the FXOS CLI using the enter ssh-host command in the system/services scope.

- prompt - You are prompted to accept or reject the host key if it is not already stored on the chassis.

- disable - (The default) The chassis accepts the host key automatically if it was not stored before.

Step 12 For the client Encryption Algorithm, check the check boxes for each allowed encryption algorithm.

Note 3des-cbc is not supported in Common Criteria. If Common Criteria mode is enabled on the FXOS chassis, you cannot use 3des-cbc as an encryption algorithm.

Step 13 For the client Key Exchange Algorithm, check the check boxes for each allowed Diffie-Hellman (DH) key exchange. The DH key exchange provides a shared secret that cannot be determined by either party alone. The key exchange is combined with a signature and the host key to provide host authentication. This key-exchange method provides explicit server authentication. For more information about using DH key-exchange methods, see RFC 4253.

Step 14 For the client Mac Algorithm, check the check boxes for each allowed integrity algorithm.

Step 15 For the client Volume Rekey Limit, set the amount of traffic in KB allowed over the connection before FXOS disconnects from the session.

Step 16 For the client Time Rekey Limit, set the minutes for how long an SSH session can be idle before FXOS disconnects the session.

Step 17 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 /system/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:


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.
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>
<thead>
<tr>
<th>Model</th>
<th>Level</th>
<th>Authentication</th>
<th>Encryption</th>
<th>What Happens</th>
</tr>
</thead>
<tbody>
<tr>
<td>v1</td>
<td>noAuthNoPriv</td>
<td>Community string</td>
<td>No</td>
<td>Uses a community string match for authentication.</td>
</tr>
<tr>
<td>v2c</td>
<td>noAuthNoPriv</td>
<td>Community string</td>
<td>No</td>
<td>Uses a community string match for authentication.</td>
</tr>
<tr>
<td>v3</td>
<td>noAuthNoPriv</td>
<td>Username</td>
<td>No</td>
<td>Uses a username match for authentication.</td>
</tr>
<tr>
<td>v3</td>
<td>authNoPriv</td>
<td>HMAC-SHA</td>
<td>No</td>
<td>Provides authentication based on the HMAC Secure Hash Algorithm (SHA).</td>
</tr>
<tr>
<td>v3</td>
<td>authPriv</td>
<td>HMAC-SHA</td>
<td>DES</td>
<td>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.</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Platform Settings &gt; SNMP.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the SNMP area, complete the following fields:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin State</td>
<td>Whether SNMP is enabled or disabled. Enable this service only if your system includes integration with an SNMP server.</td>
</tr>
</tbody>
</table>
### Creating an SNMP Trap

#### Description

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port field</td>
<td>The port on which the Firepower chassis communicates with the SNMP host. You cannot change the default port.</td>
</tr>
<tr>
<td>Community/Username field</td>
<td>The community string used for polling in SNMP v1 and v2. Note that this field is not applicable to SNMP v3. Enter an alphanumeric string between 1 and 32 characters. Do not use @ (at sign), \ (backward slash), &quot; (double quote), ? (question mark) or an empty space. The default is <code>public</code>. Note that 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.</td>
</tr>
<tr>
<td>System Administrator Name field</td>
<td>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.</td>
</tr>
<tr>
<td>Location field</td>
<td>The location of the host on which the SNMP agent (server) runs. Enter an alphanumeric string up to 510 characters.</td>
</tr>
</tbody>
</table>

#### Step 3

Click Save.

#### What to do next

Create SNMP traps and users.

---

### Creating an SNMP Trap

#### 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name field</td>
<td>The hostname or IP address of the SNMP host to which the Firepower chassis should send the trap.</td>
</tr>
</tbody>
</table>
Name | Description
--- | ---
Community/Username field | The SNMP v1 or v2 community name or the SNMP v3 username the Firepower chassis includes when it sends the trap to the SNMP host. This must be the same as the community or username 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
Type field | If you select V2 or V3 for the version, the type of trap to send. This can be one of the following:
  • Traps
  • Informs
v3 Privilege field | If you select V3 for the version, the privilege associated with the trap. This can be one of the following:
  • Auth—Authentication but no encryption
  • Noauth—No authentication or encryption
  • 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.
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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>The username assigned to the SNMP user. Enter up to 32 characters. The name must begin with a letter. Valid characters include letters, numbers, _ (underscore), . (period), @ (at sign), and - (hyphen).</td>
</tr>
<tr>
<td>Auth Type field</td>
<td>The authorization type: SHA.</td>
</tr>
<tr>
<td>Use AES-128 check box</td>
<td>If checked, this user uses AES-128 encryption.</td>
</tr>
<tr>
<td>Password field</td>
<td>The password for this user. The Firepower eXensible Operating System rejects any password that does not meet the following requirements:</td>
</tr>
<tr>
<td></td>
<td>• Must contain a minimum of 8 characters and a maximum of 80 characters.</td>
</tr>
<tr>
<td></td>
<td>• Must contain only letters, numbers, and the following characters: ~`!@#%^&amp;*()_-+[]{]};:&quot;'&lt;&gt;/</td>
</tr>
<tr>
<td></td>
<td>• Must not contain the following symbols: $ (dollar sign), ? (question mark), or = (equals sign).</td>
</tr>
<tr>
<td></td>
<td>• Must contain at least five different characters.</td>
</tr>
<tr>
<td></td>
<td>• Must not contain too many consecutively incrementing or decrementing numbers or letters. For example, the string &quot;12345&quot; has four such characters, and the string &quot;ZYXW&quot; 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.</td>
</tr>
<tr>
<td>Note</td>
<td>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>
</tbody>
</table>
### 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.

---

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Confirm Password</strong> field</td>
<td>The password again for confirmation purposes.</td>
</tr>
</tbody>
</table>
| **Privacy Password** field   | 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. |
| **Confirm Privacy Password** field | The privacy password again for confirmation purposes. |
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
```
### Creating a Certificate Request for a Key Ring

#### Creating a Certificate Request for a Key Ring with Basic Options

**Procedure**

1. **Step 1**
   - Enter security mode:
   ```
   Firepower-chassis # scope security
   ```
2. **Step 2**
   - Enter configuration mode for the key ring:
   ```
   Firepower-chassis /security # scope keyring keyring-name
   ```
3. **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}
   ```
4. **Step 4**
   - Commit the transaction:
   ```
   Firepower-chassis /security/keyring/certreq # commit-buffer
   ```
5. **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 keyring-name
Firepower-chassis /security/keyring # create certreq {ip [ipv4-addr | ipv6-v6] | subject-name name}
Firepower-chassis /security/keyring/certreq # commit-buffer
Firepower-chassis /security/keyring # show certreq
```
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/vW2rnRF8QPhKbhghLA1YpZIF
JqcYEESY11vqoLBDt45soGQG84rTLWH0s4SwcUXQ52Qf45YtJX1wylUWV4
0/re/zzTk/ZeCd565FOkWWR2Dztzu2pGA14sd761z2xt29kh78mzj6CAUVAqMBAAgg
LTAzbGqkhiG9w0BCq4xHjAcMBoGA1UDQEB/wQQMA6CBnHbWMwN1cECsEiXjAN
Bgqkh1iG9wOBAQQFAAOBgQCSxnNOgQHYGFcQWA56rQWueLTNPrndqUwZH003Teg
mhsyu4asatpylPqV9v1KZ+zspvcsx5PF1cWvG8hH8B1Ob/00KuG8kwfJ1q5aED1Av
TTyU8+Z29Of1PbRAlA718S+V8ndXrIHejqiGxlDNqoN+oCXPC5kjoXO1ZTL09H
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
Creating a Trusted Point

**Procedure**

**Step 1**
Enter security mode:

```
Firepower-chassis# scope security
```

**Step 2**
Create a trusted point:

```
Firepower-chassis /security/trustpoint
```

**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 END OF BUF to finish.

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

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.
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:

commit the transaction:

firepower-chassis /security/trustpoint # commit-buffer
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/zCCAwgCAQAwg2kxCzAjbGNVBAYTA1VTMQsCQYDVQQIExwJDAFMDQGMBBA5wDAYJKoZIhvcNAQEFBQADgY0AMIGJA...
> AoGHAHzW4nTep+g7Gz7nNaKQzAiGz6zSHRMQeOHG/remdh66u2/XAoLx7YCcYU...
> gYAItyvCsKgb/6CyQts0FvtrMC/eaAhtuK3/SINv7wd6Vz2p6ZpXgD4VBKND1...
> Ptt5CvQnNgNldvDPsXzretysOhqHmp9+CLv8FDuy1CDYfualTv1WvhevskV0j6...
> mK3ku+YiORnv6DhxOogau8r/hyI/L317lPIN1H0i3oha4=
> -----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:

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
```

### 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**

1. Choose **Platform Settings** &gt; HTTPS.
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.
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**

1. Enter security mode:
Deleting a Trusted Point

**Before you begin**
Ensure that the trusted point is not used by a key ring.

**Procedure**

**Step 1**
Enter 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

AAA is a set of services for controlling access to computer resources, enforcing policies, assessing usage, and providing the information necessary to bill for services. These processes are considered important for effective network management and security.

Authentication

Authentication provides a way to identify a user, typically by having the user enter a valid username and valid password before access is granted. The AAA server compares a user's authentication credentials with other user credentials stored in a database. If the credentials match, 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 a user is permitted to access. After a user is authenticated, that 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.

**AAA Servers**

The AAA server is a network server that is used for access control. 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.

**Local Database Support**

The Firepower chassis maintains a local database that you can populate with user profiles. You can use a local database instead of AAA servers to provide user authentication, authorization, and accounting.

**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**

1. Choose Platform Settings > AAA.
Step 2  Click the LDAP tab.

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Timeout</strong></td>
<td>The length of time in seconds the system should 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.</td>
</tr>
<tr>
<td><strong>Attribute</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Base DN</strong></td>
<td>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 username. The length of the base DN can be set to a maximum of 255 characters minus the length of $userid, where $userid identifies the remote user attempting to access the Firepower chassis using LDAP authentication. This property is required. If you do not specify a base DN on this tab then you must specify one for each LDAP provider that you define.</td>
</tr>
<tr>
<td><strong>Filter</strong></td>
<td>The LDAP search is restricted to those user names that match the defined filter. 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.</td>
</tr>
</tbody>
</table>

Step 4  Click Save.

What to do next

Create an LDAP provider.

Creating an LDAP Provider

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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname/FQDN (or IP Address) field</td>
<td>The hostname or IP address on which the LDAP provider resides. If SSL is enabled, this field must exactly match a Common Name (CN) in the security certificate of the LDAP database.</td>
</tr>
<tr>
<td>Order field</td>
<td>The order in which the Firepower eXtensible Operating System uses this provider to authenticate users. Enter an integer between 1 and 16, or enter <strong>lowest-available</strong> 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.</td>
</tr>
<tr>
<td>Bind DN field</td>
<td>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.</td>
</tr>
<tr>
<td>Base DN field</td>
<td>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 username. 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 <strong>LDAP</strong> tab.</td>
</tr>
<tr>
<td>Port field</td>
<td>The port through which Firepower Chassis Manager or the FXOS CLI communicates with the LDAP database. The standard port number is 389.</td>
</tr>
<tr>
<td>Enable SSL check box</td>
<td>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.</td>
</tr>
<tr>
<td>Filter field</td>
<td>The LDAP search is restricted to those user names that match the defined filter. This value is required unless a default filter has been set on the <strong>LDAP</strong> tab.</td>
</tr>
<tr>
<td>Attribute field</td>
<td>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 <strong>LDAP</strong> tab.</td>
</tr>
</tbody>
</table>
### Name | Description
--- | ---
**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 purposes.

**Timeout field** | The length of time in seconds the system should 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.

---

### 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 the default setting.
Creating a RADIUS Provider

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Timeout</strong> field</td>
<td>The length of time in seconds the system should 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.</td>
</tr>
<tr>
<td><strong>Retries</strong> field</td>
<td>The number of times to retry the connection before the request is considered to have failed.</td>
</tr>
</tbody>
</table>

**Step 4** Click **Save**.

### What to do next

Create a RADIUS provider.

Creating a RADIUS Provider

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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hostname/FDQN (or IP Address)</strong> field</td>
<td>The hostname or IP address on which the RADIUS provider resides.</td>
</tr>
<tr>
<td><strong>Order</strong> field</td>
<td>The order in which the Firepower eXtensible Operating System uses this provider to authenticate users. Enter an integer between 1 and 16, or enter <strong>lowest-available</strong> 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.</td>
</tr>
<tr>
<td><strong>Key</strong> field</td>
<td>The SSL encryption key for the database.</td>
</tr>
</tbody>
</table>
The SSL encryption key repeated for confirmation purposes.

**Confirm Key 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.

**Authorization Port field**

The length of time in seconds the system should 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.

**Timeout 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.

**Retries field**

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 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.

**Procedure**

**Step 1** Choose Platform Settings > AAA.
**Step 2** Click the TACACS tab.

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Timeout field</strong></td>
<td>The length of time in seconds the system should 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.</td>
</tr>
</tbody>
</table>

**Step 4** Click Save.

---

**What to do next**

Create a TACACS+ provider.

---

**Creating a TACACS+ Provider**

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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hostname/FDQN (or IP Address) field</strong></td>
<td>The hostname or IP address on which the TACACS+ provider resides.</td>
</tr>
<tr>
<td><strong>Order field</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Key field</strong></td>
<td>The SSL encryption key for the database.</td>
</tr>
<tr>
<td><strong>Confirm Key field</strong></td>
<td>The SSL encryption key repeated for confirmation purposes.</td>
</tr>
<tr>
<td><strong>Port field</strong></td>
<td>The port through which Firepower Chassis Manager or the FXOS CLI communicates with the TACACS+ database. Enter an integer between 1 and 65535. The default port is 49.</td>
</tr>
</tbody>
</table>
Deleting a TACACS+ Provider

**Procedure**

1. Choose **Platform Settings > AAA**.
2. Click the **TACACS** tab.
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**

1. Choose **Platform Settings > Syslog**.
2. Configure Local Destinations:
   a) Click the **Local Destinations** tab.
   b) On the **Local Destinations** tab, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td></td>
</tr>
<tr>
<td>Section</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Syslog

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Admin State</strong></td>
<td>Whether the Firepower chassis displays syslog messages on the console. Check the <strong>Enable</strong> check box if you want to have syslog messages displayed on the console as well as added to the log. If the <strong>Enable</strong> check box is unchecked, syslog messages are added to the log but are not displayed on the console.</td>
</tr>
<tr>
<td><strong>Level</strong></td>
<td>If you checked the <strong>Enable</strong> check box for <strong>Console - Admin State</strong>, 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:</td>
</tr>
<tr>
<td></td>
<td>• Emergencies</td>
</tr>
<tr>
<td></td>
<td>• Alerts</td>
</tr>
<tr>
<td></td>
<td>• Critical</td>
</tr>
<tr>
<td><strong>Monitor</strong></td>
<td>Whether the Firepower chassis displays syslog messages on the monitor. Check the <strong>Enable</strong> check box if you want to have syslog messages displayed on the monitor as well as added to the log. If the <strong>Enable</strong> check box is unchecked, syslog messages are added to the log but are not displayed on the monitor.</td>
</tr>
<tr>
<td><strong>Level</strong> drop-down list</td>
<td>If you checked the <strong>Enable</strong> check box for <strong>Monitor - Admin State</strong>, 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:</td>
</tr>
<tr>
<td></td>
<td>• Emergencies</td>
</tr>
<tr>
<td></td>
<td>• Alerts</td>
</tr>
<tr>
<td></td>
<td>• Critical</td>
</tr>
<tr>
<td></td>
<td>• Errors</td>
</tr>
<tr>
<td></td>
<td>• Warnings</td>
</tr>
<tr>
<td></td>
<td>• Notifications</td>
</tr>
<tr>
<td></td>
<td>• Information</td>
</tr>
<tr>
<td></td>
<td>• Debugging</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Admin State</strong></td>
<td>Check the <strong>Enable</strong> check box if you want to have syslog messages stored in a remote log file.</td>
</tr>
<tr>
<td><strong>Level</strong> drop-down list</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• Emergencies</td>
</tr>
<tr>
<td></td>
<td>• Alerts</td>
</tr>
<tr>
<td></td>
<td>• Critical</td>
</tr>
<tr>
<td></td>
<td>• Errors</td>
</tr>
<tr>
<td></td>
<td>• Warnings</td>
</tr>
<tr>
<td></td>
<td>• Notifications</td>
</tr>
<tr>
<td></td>
<td>• Information</td>
</tr>
<tr>
<td></td>
<td>• Debugging</td>
</tr>
</tbody>
</table>

| **Hostname/IP Address** field | The hostname or IP address on which the remote log file resides. 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:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Faults Admin State</td>
<td>Whether system fault logging is enabled or not. If the Enable check box is checked, the Firepower chassis logs all system faults.</td>
</tr>
<tr>
<td>Audits Admin State</td>
<td>Whether audit logging is enabled or not. If the Enable check box is checked, the Firepower chassis logs all audit log events.</td>
</tr>
<tr>
<td>Events Admin State</td>
<td>Whether system event logging is enabled or not. If the Enable check box is checked, the Firepower chassis logs all system events.</td>
</tr>
</tbody>
</table>

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, on page 73
- Guidelines and Limitations for Firepower Interfaces, on page 74
- Configure Interfaces, on page 74
- Monitoring Interfaces, on page 77

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. See also Changing the Management IP Address, on page 37. 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—Data interfaces cannot be shared between logical devices.
- Mgmt—Use management interfaces to manage application instances. They 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 information about the separate chassis management interface, see Chassis Management Interface, on page 73.

• Cluster—Special interface type used for a clustered logical device. This type is automatically assigned to the cluster control link for inter-unit cluster communications. By default, the cluster control link is automatically created on Port-channel 48.

**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**

**Inline Sets for FTD**

- Supported for physical interfaces only (both regular and breakout ports); EtherChannels are not supported.
- Link state propagation is not supported.

**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, edit interface properties, and configure breakout ports.

**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 (●) so that it changes to the enabled slider (✔). 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 enabled slider (✔) so that it changes to the disabled slider (●). 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 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, or 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 type. The Link Aggregation Control Protocol (LACP) aggregates interfaces by exchanging the Link Aggregation Control Protocol Data Units (LACPDUs) between two network devices.

The Firepower 9300 chassis only supports EtherChannels in Active LACP mode so that each member interface sends and receives LACP updates. An active EtherChannel can establish connectivity with either an active or a passive EtherChannel. You should use the active mode unless you need to minimize the amount of LACP traffic.

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.

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 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 configure an EtherChannel with a different ID and choose the Cluster type for the interface. 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, or Cluster.

Do not choose the Cluster type unless you want to use this port-channel as the cluster control link instead of the default.

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 of the same type and speed.

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.
Logical Devices

- About Logical Devices, on page 79
- Requirements and Prerequisites for Logical Devices, on page 80
- Guidelines and Limitations for Logical Devices, on page 80
- Add a Standalone Logical Device, on page 81
- Add a High Availability Pair, on page 82
- Add a Cluster, on page 83
- Manage Logical Devices, on page 86
- Logical Devices Page, on page 92
- History for Logical Devices, on page 94

About Logical Devices

A logical device lets you run one application instance (either ASA or Firepower Threat Defense) and also one optional decorator application (Radware DefensePro) to form a service chain.

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.

Note

For the Firepower 9300, you must install the same application instance type (ASA or Firepower Threat Defense) on all modules in the chassis; different types are not supported at this time. Note that modules can run different versions of an application instance type.

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 module application instances belong to a single logical device.
Requirements and Prerequisites for Logical Devices

See the following sections for requirements and prerequisites.

Requirements and Prerequisites for Clustering

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 a list of supported switches, see Cisco FXOS Compatibility.

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. For the ASA, you can change the firewall mode to transparent after you deploy. See Change the ASA to Transparent Firewall Mode, on page 88.

High Availability

- Configure high availability within the application configuration.
- You can use any data interfaces as the failover and state links.
- For more information, see the application configuration guide chapter for High Availability

Context Mode

- Multiple context mode is only supported on the ASA.
- Enable multiple context mode in the ASA after you deploy.
Clustering Guidelines and Limitations

- 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 control link uses Port-channel 48.

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 82.

Add a Standalone ASA

Standalone logical devices work either alone or in a High Availability pair. On multiple module devices, like the Firepower 9300, 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. To change the ASA to transparent firewall mode, complete this procedure, and then see Change the ASA to Transparent Firewall Mode, on page 88.

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 (see Downloading Images from Cisco.com, on page 32), and then upload that image to the Firepower 9300 chassis (see Uploading an Image to the Firepower Security Appliance, on page 32).
- 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 interface that is used only for chassis management (and that appears at the top of the Interfaces tab as MGMT).

Procedure

Step 1
Choose Logical Devices.

The Logical Devices page shows a list of logical devices on the chassis.

Step 2
Click Add Device.

The Add Device dialog box appears.

Step 3
For the Device Name, provide a name for the logical device.
This name is used by the Firepower 9300 chassis supervisor to configure management settings and to assign interfaces; it is not the device name used in the security module/engine configuration.

Step 4  For the Template, choose Cisco Adaptive Security Appliance.
Step 5  Choose the Image Version.
Step 6  For the Device Mode, click the Standalone radio button.
Step 7  Click OK.
You see the Provisioning - device name window.
Step 8  Expand the Data Ports area, and click each port that you want to assign to the device.
Step 9  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 change most values in the application CLI configuration.
Step 10 On the General Information tab, complete the following:
   a) (On multiple module devices, like 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.
   c) Choose the management interface Address Type, IPv4 only, IPv6 only, or IPv4 and IPv6.
   d) Configure the Management IP address.
   e) Enter a Network Mask or Prefix Length.
   f) Enter a Network Gateway address.
Step 11 Click the Settings tab.
Step 12 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 13 Click OK to close the configuration dialog box.
Step 14 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 specified security module/engine.

---

**Add a High Availability Pair**

ASA 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**

- For High Availability system requirements, see the application configuration guide chapter for High Availability.
Procedure

**Step 1**
Each logical device should be on a separate chassis; intra-chassis High Availability for the Firepower 9300 is not recommended and may not be supported.

**Step 2**
Allocate the same interfaces to each logical device.

**Step 3**
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 4**
Enable High Availability on the logical devices.

**Step 5**
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.

**Note**
For the ASA, if you remove an interface in FXOS (for example, if you remove a network module, remove an EtherChannel, or reassign an interface to an EtherChannel), then the ASA configuration retains the original commands so that you can make any necessary adjustments; removing an interface from the configuration can have wide effects. You can manually remove the old interface configuration in the ASA OS.

---

**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.

**Note**
The Firepower 9300 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.
- Creates the cluster bootstrap configuration within the application.
When you deploy the cluster, the Firepower 9300 chassis supervisor pushes a minimal bootstrap configuration to each unit that includes the cluster name, cluster control link interface, and other cluster settings.

• Assigns data interfaces to the cluster as Spanned interfaces.

For intra-chassis clustering, spanned interfaces are not limited to EtherChannels. 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.

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.

Cluster control link traffic includes both control and data traffic.

**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.

**Add an ASA Cluster**

You can add a single Firepower 9300 chassis as an intra-chassis cluster.
Create an ASA Cluster

Deploy the cluster on 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.

You can 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.

Before you begin

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

- On the Interfaces tab, 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.

Procedure

Step 1  Add at least one Data type interface or EtherChannel (also known as a port-channel) before you deploy the cluster. See Add an EtherChannel (Port Channel), on page 76 or Configure a Physical Interface, on page 75. You can also add data interfaces to the cluster after you deploy it.

Step 2  Add a Management type interface or EtherChannel. See Add an EtherChannel (Port Channel), on page 76 or Configure a Physical Interface, on page 75.

Step 3  Choose Logical Devices.

The Logical Devices page shows a list of logical devices on the chassis.

Step 4  Click Add Device.

The Add Device dialog box appears.

Step 5  For the Device Name, provide a name for the logical device.

This name is used by the Firepower 9300 chassis supervisor to configure management settings and to assign interfaces; it is not the device name used in the security module/engine configuration.

Step 6  For the Template, choose Cisco Adaptive Security Appliance.

Step 7  Choose the ASA Image Version.

Step 8  For the Device Mode, click the Cluster radio button.

Step 9  Click OK.

If you have any standalone devices configured, you are prompted to replace them with a new cluster. You see the Provisioning - device name window.

All interfaces are assigned to the cluster by default.

Step 10  Click the device icon in the center of the screen.

The ASA Configuration dialog box appears with the Cluster Information tab selected.
Step 11  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.

Step 12  Set the **Cluster Group Name**, which is the cluster group name in the security module configuration.

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

Step 13  Click **Management Interface** and choose the management interface you created earlier.

Step 14  Choose the **Address Type** for the management interface.

This information is used to configure a management interface in the security module configuration.

a) In the **Management IP Pool** field, 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 master 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.

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

c) Enter a **Network Gateway**.

d) Enter a **Virtual IP address**.

This IP address must be on the same network as the cluster pool addresses, but not be part of the pool.

Step 15  Click the **Settings** tab.

Step 16  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 17  Click **OK** to close the ASA Configuration dialog box.

Step 18  Click **Save**.

The Firepower 9300 chassis supervisor deploys the cluster by downloading the specified software version and pushing the cluster bootstrap configuration and management interface settings to each security module.

Step 19  Connect to the master unit ASA to customize your clustering configuration.

---

**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.

`connect asa`

**Example:**

```
Firepower-module1> connect asa
Connecting to asa(asal) console... hit Ctrl + A + D to return to bootCLI
[...]
asa>
```

**Example:**

```
Firepower-module1> connect ftd
Connecting to ftd(ftd-native) console... enter exit to return to bootCLI
>
```

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

- ASA—Enter Ctrl-a, d

You might want to use the FXOS module CLI for troubleshooting purposes.

**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
```
Example

The following example connects to an ASA on security module 1 and then exits back to the supervisor level of the FXOS CLI.

```
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> connect asa
asa> ~
telnet> quit
Connection closed.
Firepower#
```

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 86. 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: 9f031d8b 60d9fa8c 1d939f84 747356b9
Beginning configuration replication to Slave unit-1-2
   End Configuration Replication to slave.

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  Click Save to redeploy the configuration to the ASA.
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 a Firepower Threat Defense logical device. You can then sync the interface configuration in the Firepower Management Center.

Before you begin

• Configure your interfaces, and add any EtherChannels according to Configure a Physical Interface, on page 75 and Add an EtherChannel (Port Channel), on page 76.
  
• You can edit the membership of an allocated EtherChannel without affecting the logical device or requiring a sync on the Firepower Management Center.

• 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 Firepower Threat Defense device reboots (management interface changes cause a reboot), and you sync the configuration in the Firepower Management Center, 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 Firepower Management Center. We recommend that you make the interface changes on the slave/standby unit(s) first, and then on the master/active unit. Note that new interfaces are added in an administratively down state, so they do not affect interface monitoring.
**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Firepower Chassis Manager, choose Logical Devices.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click the Edit icon at the top right to edit the logical device.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Unallocate a data interface by de-selecting the interface in the Data Ports area.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Allocate a new data interface by selecting the interface in the Data Ports area.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Replace the management or eventing interface:</td>
</tr>
</tbody>
</table>

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/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.

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Click Save.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 7</td>
<td>Log into the Firepower Management Center.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Select Devices &gt; Device Management and click the edit icon (📝) for your FTD device. The Interfaces tab is selected by default.</td>
</tr>
<tr>
<td>Step 9</td>
<td>Click the Sync Interfaces from device button on the top left of the Interfaces tab.</td>
</tr>
<tr>
<td>Step 10</td>
<td>Click Save.</td>
</tr>
</tbody>
</table>

You can now click Deploy and deploy the policy to assigned devices. The changes are not active until you deploy them.

---

**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.

**Before you begin**

- Configure your interfaces and add any EtherChannels according to Configure a Physical Interface, on page 75 and Add an EtherChannel (Port Channel), on page 76.

- You can edit the membership of an allocated EtherChannel without impacting the logical device.

- 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 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), then the ASA configuration retains the original commands so that you can make any necessary adjustments; removing an interface from the configuration can have wide effects. You can manually remove the old interface configuration in the ASA OS.

• 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 slave/standby unit(s) first, and then on the master/active unit. New interfaces are added in an administratively down state, so they do not affect interface monitoring.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Firepower Chassis Manager, choose Logical Devices.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the Edit icon at the top right to edit the logical device.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Unallocate a data interface by de-selecting the interface in the Data Ports area.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Allocate a new data interface by selecting the interface in the Data Ports area.</td>
</tr>
</tbody>
</table>
| Step 5 | Replace the management interface:  
  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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Firepower Chassis Manager, choose Logical Devices.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the Edit icon at the top right to edit the logical device.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the device icon in the center of the page.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Modify the logical device settings as required.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click OK.</td>
</tr>
</tbody>
</table>
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, master or slave.
• 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.
### History for Logical Devices

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intra-chassis Clustering for the Cisco ASA</td>
<td>1.1.1</td>
<td>You can cluster all ASA security modules within the Firepower 9300 chassis.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>We introduced the following screen: Logical Devices &gt; Configuration</td>
</tr>
</tbody>
</table>
INDEX

A
AAA 62, 63, 65, 66, 67, 68, 69
   LDAP providers 62, 63, 65
   RADIUS providers 65, 66, 67
   TACACS+ providers 67, 68, 69
accessing the command line interface 9
accounts 22, 29
   locally authenticated 22, 29
asa 33, 81, 85, 86
   connecting to 86
   creating a cluster 85
   creating a clustered 81
   creating a standalone asa logical device 81
   exiting from connection 86
   updating image version 33
asa images 31, 32
   about 31
   downloading from Cisco.com 32
   uploading to the Firepower security appliance 32
authentication 23
   default 23
authNoPriv 44
authPriv 44

B
breakout cables 77
   configuring 77
breakout ports 77

C
call home 15
   configure http proxy 15
certificate 50
   about 50
chassis 2, 5
   initial configuration 5
   monitoring status 2
chassis manager 1
   user interface overview 1
Cisco Secure Package 31, 32
   about 31
   downloading from Cisco.com 32

Cisco Secure Package (continued)
   uploading to the Firepower security appliance 32
cli, See command line interface
clusters 81, 83, 85
   about 83
   creating 81, 85
command line interface 9
   accessing 9
communication services 45, 51, 52, 53, 55, 56
   HTTPS 51, 52, 53, 55, 56
   SNMP 45
community, SNMP 45
   configuring 51, 52, 53, 55, 56
   HTTPS 51, 52, 53, 55, 56
   connecting to a logical device 86
console 25
   timeout 25
CSP, See Cisco Secure Package

D
date 40
   setting manually 40
date and time 39
   configuring 39
DNS 72

E
enabling 45
SNMP 45
exiting from logical device connection 86

F
Firepower chassis 2, 5
   initial configuration 5
   monitoring status 2
Firepower Chassis Manager 1, 8
   logging in or out 8
   user interface overview 1
Firepower eXtensible OS 33
   upgrading the platform bundle 33
Firepower platform bundle  31, 32, 33
  about  31
downloading from Cisco.com  32
  upgrading  33
uploading to the Firepower security appliance  32
  verifying integrity  32
Firepower security appliance  1
  overview  1
firmware  34
  upgrading  34
fpga  34
  upgrading  34
FXOS chassis, See Firepower chassis
H
  high-level task list  5
history, passwords  22
http proxy  15
  configuring  15
HTTPS  8, 29, 51, 52, 53, 55, 56, 58, 59, 61
  certificate request  52, 53
  changing port  59
  configuring  58
  creating key ring  51
  disabling  61
  importing certificate  56
  logging in or out  8
  regenerating key ring  51
timeout  25
  trusted point  55
I
  image version  33
  updating  33
images  31, 32, 33
  downloading from Cisco.com  32
  managing  31
upgrading the Firepower eXtensible Operating System platform bundle  33
uploading to the Firepower security appliance  32
  verifying integrity  32
informs  43
  about  43
initial configuration  5
  configuring  75
  properties  75
K
  key ring  50, 51, 52, 53, 55, 56, 59
  about  50
  certificate request  52, 53
  key ring (continued)
    creating  51
    deleting  59
    importing certificate  56
    regenerating  51
    trusted point  55
L
  LDAP  62, 63, 65
  LDAP providers  63, 65
    creating  63
    deleting  65
license  15
  registering  15
license authority  15
  locally authenticated users  22, 29
    clearing password history  29
    password profile  22
logging in or out  8
logical devices  33, 81, 85, 86, 92
  connecting to  86
  creating a cluster  81, 85
  creating a standalone  81
  exiting from connection  86
  understanding  92
updating image version  33
M
  management IP address  37
    changing  37
  monitoring chassis status  2
N
  noAuthNoPriv  44
NTP  39, 40
  adding  39
  configuring  39
  deleting  40
P
  password profile  22, 29
    about  22
    clearing password history  29
passwords  19, 22, 23
  change interval  22
  guidelines  19
  history count  22
  strength check  23
PKI  50
  platform bundle  31, 32, 33
    about  31
platform bundle (continued)
downloading from Cisco.com 32
upgrading 33
uploading to the Firepower security appliance 32
verifying integrity 32
port channels 76
configuring 76
profiles 22
password 22

R
RADIUS 65, 66, 67
RADIUS providers 66, 67
  creating 66
deleting 67
registering a license 15
rommon 34
  upgrading 34
RSA 50

S
session timeout 25
smart call home 15
  configure http proxy 15
SNMP 43, 44, 45, 46, 47, 48, 49
  about 43
  community 45
  enabling 45
  notifications 43
  privileges 44
  security levels 44
  support 43, 45
traps 46, 47
  creating 46
deleting 47
users 48, 49
  creating 48
deleting 49
Version 3 security features 44
SNMPv3 44
  security features 44
SSH 25, 40
  configuring 40
timeout 25
syslog 69
  configuring local destinations 69
  configuring local sources 69
  configuring remote destinations 69
system 5
  initial configuration 5

T
TACACS+ 67, 68, 69
TACACS+ providers 68, 69
  creating 68
deleting 69
task flow 5
telnet 25, 42
  configuring 42
timeout 25
time 40
  setting manually 40
time zone 39, 40
  setting 39, 40
timeout 25
  console 25
  HTTPS, SSH, and Telnet 25
traps 43, 46, 47
  about 43
  creating 46
deleting 47
trusted points 50, 55, 60
  about 50
  creating 55
deleting 60

U
upgrading the firmware 34
user accounts 22, 29
  password profile 22, 29
user interface 1
  overview 1
users 17, 18, 19, 22, 23, 27, 28, 29, 48, 49
  activating 28
  creating 27
  deactivating 28
  default authentication 23
deleting 28
  locally authenticated 22, 29
  managing 17
  naming guidelines 18
  password guidelines 19
  roles 22
  settings 23
  SNMP 48, 49