THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2015 Cisco Systems, Inc. All rights reserved.
User Management  25
  User Accounts  25
  Guidelines for Usernames  26
  Guidelines for Passwords  27
  Guidelines for Remote Authentication  27
  User Roles  30
  Password Profile for LocallyAuthenticated Users  30
  Select the Default Authentication Service  31
  Configuring the Session Timeout  33
  Configuring the Role Policy for Remote Users  33
  Enabling Password Strength Check for LocallyAuthenticated Users  34
  Set the Maximum Number of Login Attempts  35
  Configuring the Maximum Number of Password Changes for a Change Interval  36
  Configuring a No Change Interval for Passwords  37
  Configuring the Password History Count  38
  Creating a Local User Account  38
  Deleting a Local User Account  41
  Activating or Deactivating a Local User Account  41
  Clearing the Password History for a LocallyAuthenticated User  42
CHAPTER 6

Image Management 43
  About Image Management 43
  Downloading Images from Cisco.com 44
  Downloading a Firepower eXtensible Operating System Software Image to the Firepower 9300 chassis 44
  Verifying the Integrity of an Image 45
  Upgrading the Firepower eXtensible Operating System Platform Bundle 46
  Downloading a Logical Device Software Image to the Firepower 9300 chassis 47
  Updating the Image Version for a Logical Device 49
  Firmware Upgrade 50

CHAPTER 7

Platform Settings 55
  Changing the Management IP Address 55
  Setting the Date and Time 57
    Setting the Time Zone 57
    Setting the Date and Time Using NTP 59
  Deleting an NTP Server 60
  Setting the Date and Time Manually 61
  Configuring SSH 62
  Configuring Telnet 62
  Configuring SNMP 63
    About SNMP 63
    SNMP Notifications 64
    SNMP Security Levels and Privileges 64
    Supported Combinations of SNMP Security Models and Levels 65
    SNMPv3 Security Features 65
    SNMP Support 65
    Enabling SNMP and Configuring SNMP Properties 66
    Creating an SNMP Trap 67
    Deleting an SNMP Trap 69
    Creating an SNMPv3 User 69
    Deleting an SNMPv3 User 71
  Configuring HTTPS 71
Certificates, Key Rings, and Trusted Points  72
Creating a Key Ring  72
Regenerating the Default Key Ring  73
Creating a Certificate Request for a Key Ring  74
  Creating a Certificate Request for a Key Ring with Basic Options  74
  Creating a Certificate Request for a Key Ring with Advanced Options  75
Creating a Trusted Point  77
Importing a Certificate into a Key Ring  78
Configuring HTTPS  79
Changing the HTTPS Port  81
Deleting a Key Ring  82
Deleting a Trusted Point  82
Disabling HTTPS  83
Configuring AAA  83
  About AAA  84
  Configuring LDAP Providers  85
    Configuring Properties for LDAP Providers  85
    Creating an LDAP Provider  86
    Deleting an LDAP Provider  89
  Configuring RADIUS Providers  89
    Configuring Properties for RADIUS Providers  89
    Creating a RADIUS Provider  90
    Deleting a RADIUS Provider  91
  Configuring TACACS+ Providers  92
    Configuring Properties for TACACS+ Providers  92
    Creating a TACACS+ Provider  93
    Deleting a TACACS+ Provider  94
Configuring Syslog  94
Configuring DNS Servers  97

CHAPTER 8  Interface Management  99
  About Firepower Interfaces  99
    Chassis Management Interface  99
    Interface Types  99
Logical Devices 109

CHAPTER 9

About Logical Devices 109

Standalone and Clustered Logical Devices 109

Requirements and Prerequisites for Logical Devices 110

Requirements and Prerequisites for Clustering 110

Guidelines and Limitations for Logical Devices 111

General Guidelines and Limitations 111

Clustering Guidelines and Limitations 112

Add a Standalone Logical Device 115

Add a Standalone ASA 115

Add a High Availability Pair 120

Add a Cluster 121

About Clustering on the Firepower 9300 Chassis 121

Primary and Secondary Unit Roles 121

Cluster Control Link 122

Management Network 123

Management Interface 123

Spanned EtherChannels 124

Inter-Site Clustering 124

Add an ASA Cluster 125

Create an ASA Cluster 125

Add More Cluster Members 132

Manage Logical Devices 132

Connect to the Console of the Application 132

Delete a Logical Device 134
# Contents

## CHAPTER 10

**Configuration Import/Export** 143  
About Configuration Import/Export 143  
Exporting an FXOS Configuration File 144  
Scheduling Automatic Configuration Export 145  
Setting a Configuration Export Reminder 147  
Importing a Configuration File 148

## CHAPTER 11

**Packet Capture** 151  
Packet Capture 151  
Backplane Port Mappings 151  
Guidelines and Limitations for Packet Capture 152  
Creating or Editing a Packet Capture Session 152  
Configuring Filters for Packet Capture 154  
Starting and Stopping a Packet Capture Session 155  
Downloading a Packet Capture File 156
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.
About the Firepower Security Appliance
CLI Overview

- Managed Objects, on page 3
- Command Modes, on page 3
- Object Commands, on page 5
- Complete a Command, on page 6
- Command History, on page 6
- Commit, Discard, and View Pending Commands, on page 6
- Inline Help for the CLI, on page 7
- CLI Session Limits, on page 7

Managed Objects

The Firepower eXtensible Operating System (FXOS) uses a managed object model, where managed objects are abstract representations of physical or logical entities that can be managed. For example, chassis, security modules, network modules, ports, and processors are physical entities represented as managed objects, and licenses, user roles, and platform policies are logical entities represented as managed objects.

Managed objects may have one or more associated properties that can be configured.

Command Modes

The CLI is organized into a hierarchy of command modes, with EXEC mode being the highest-level mode of the hierarchy. Higher-level modes branch into lower-level modes. You use create, enter, and scope commands to move from higher-level modes to modes in the next lower level, and you use the up command to move up one level in the mode hierarchy. You can also use the top command to move to the top level in the mode hierarchy.

Note

Most command modes are associated with managed objects, so you must create an object before you can access the mode associated with that object. You use create and enter commands to create managed objects for the modes being accessed. The scope commands do not create managed objects and can only access modes for which managed objects already exist.
Each mode contains a set of commands that can be entered in that mode. Most of the commands available in each mode pertain to the associated managed object.

The CLI prompt for each mode shows the full path down the mode hierarchy to the current mode. This helps you to determine where you are in the command mode hierarchy, and it can be an invaluable tool when you need to navigate through the hierarchy.

The following table lists the main command modes, the commands used to access each mode, and the CLI prompt associated with each mode.

<table>
<thead>
<tr>
<th>Mode Name</th>
<th>Commands Used to Access</th>
<th>Mode Prompt</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXEC</td>
<td>top command from any mode</td>
<td>#</td>
</tr>
<tr>
<td>Adapter</td>
<td>scope adapter command from EXEC mode</td>
<td>/adapter #</td>
</tr>
<tr>
<td>Cabling</td>
<td>scope cabling command from EXEC mode</td>
<td>/cabling #</td>
</tr>
<tr>
<td>Chassis</td>
<td>scope chassis command from EXEC mode</td>
<td>/chassis #</td>
</tr>
<tr>
<td>Ethernet server domain</td>
<td>scope eth-server command from EXEC mode; this command and all subcommands are currently not supported</td>
<td>/eth-server #</td>
</tr>
<tr>
<td>Ethernet uplink</td>
<td>scope eth-uplink command from EXEC mode</td>
<td>/eth-uplink #</td>
</tr>
<tr>
<td>Fabric interconnect</td>
<td>scope fabric-interconnect command from EXEC mode</td>
<td>/fabric-interconnect #</td>
</tr>
<tr>
<td>Firmware</td>
<td>scope firmware command from EXEC mode</td>
<td>/firmware #</td>
</tr>
<tr>
<td>Host Ethernet interface</td>
<td>scope host-eth-if command from EXEC mode</td>
<td>/host-eth-if #</td>
</tr>
<tr>
<td>License</td>
<td>scope license command from EXEC mode</td>
<td>/license #</td>
</tr>
<tr>
<td>Monitoring</td>
<td>scope monitoring command from EXEC mode</td>
<td>/monitoring #</td>
</tr>
<tr>
<td>Organization</td>
<td>scope org command from EXEC mode</td>
<td>/org #</td>
</tr>
<tr>
<td>Packet capture</td>
<td>scope packet-capture command from EXEC mode</td>
<td>/packet-capture #</td>
</tr>
<tr>
<td>Security</td>
<td>scope security command from EXEC mode</td>
<td>/security #</td>
</tr>
<tr>
<td>Mode Name</td>
<td>Commands Used to Access</td>
<td>Mode Prompt</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Server</td>
<td><code>scope server</code> command from EXEC mode</td>
<td><code>/server #</code></td>
</tr>
<tr>
<td>Service profile</td>
<td><code>scope service-profile</code> command from EXEC mode</td>
<td><code>/service-profile #</code></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Do not alter or configure service profiles; that is, do not use the <code>create</code>, <code>set</code>, or <code>delete</code> subcommand sets.</td>
<td></td>
</tr>
<tr>
<td>SSA</td>
<td><code>scope ssa</code> command from EXEC mode</td>
<td><code>/ssa #</code></td>
</tr>
<tr>
<td>System</td>
<td><code>scope system</code> command from EXEC mode</td>
<td><code>/system #</code></td>
</tr>
<tr>
<td>Virtual HBA</td>
<td><code>scope vhba</code> command from EXEC mode</td>
<td><code>/vhba #</code></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This command and all subcommands are currently not supported.</td>
<td></td>
</tr>
<tr>
<td>Virtual NIC</td>
<td><code>scope vnic</code> command from EXEC mode</td>
<td><code>/vnic #</code></td>
</tr>
</tbody>
</table>

**Object Commands**

Four general commands are available for object management:

- `create object`
- `delete object`
- `enter object`
- `scope object`

You can use the `scope` command with any managed object, whether a permanent object or a user-instantiated object. The other commands allow you to create and manage user-instantiated objects. For every `create object` command, a corresponding `delete object` and `enter object` command exists.

In the management of user-instantiated objects, the behavior of these commands depends on whether the object exists, as described in the following tables:

**Table 2: Command Behavior If The Object Does Not Exist**

<table>
<thead>
<tr>
<th>Command</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>create object</code></td>
<td>The object is created and its configuration mode, if applicable, is entered.</td>
</tr>
<tr>
<td><code>delete object</code></td>
<td>An error message is generated.</td>
</tr>
<tr>
<td><code>enter object</code></td>
<td>The object is created and its configuration mode, if applicable, is entered.</td>
</tr>
<tr>
<td><code>scope object</code></td>
<td>An error message is generated.</td>
</tr>
</tbody>
</table>
### Complete a Command

You can use the Tab key in any mode to complete a command. Partially typing a command name and pressing Tab causes the command to be displayed in full or to the point where you must enter another keyword or an argument value.

### Command History

The CLI stores all commands used in the current session. You can step through the previously used commands by using the up-arrow or down-arrow keys. The up-arrow key moves to the previous command in the history, and the down-arrow key moves to the next command in the history. When you get to the end of the history, pressing the down-arrow key does nothing.

You can enter any command in the history again by stepping through the history to recall that command and then pressing Enter. The command is entered as if you had manually typed it. You can also recall a command and change it before you press Enter.

### Commit, Discard, and View Pending Commands

When you enter a configuration command in the CLI, the command is not applied until you enter the commit-buffer command. Until committed, a configuration command is pending and can be discarded by entering a discard-buffer command.

You can accumulate pending changes in multiple command modes and apply them together with a single commit-buffer command. You can view the pending commands by entering the show configuration pending command in any command mode.

---

**Note**

All pending commands are checked for validity. However, if any queued command fails during commit, the remaining commands are applied; failed commands are reported in an error message.

While any commands are pending, an asterisk (*) appears before the command prompt. The asterisk disappears when you enter the commit-buffer command.

The following example shows how the prompts change during the command entry process:

---

**Table 3: Command Behavior If The Object Exists**

<table>
<thead>
<tr>
<th>Command</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>create object</td>
<td>An error message is generated.</td>
</tr>
<tr>
<td>delete object</td>
<td>The object is deleted.</td>
</tr>
<tr>
<td>enter object</td>
<td>The configuration mode, if applicable, of the object is entered.</td>
</tr>
<tr>
<td>scope object</td>
<td>The configuration mode of the object is entered.</td>
</tr>
</tbody>
</table>
Firepower# scope system
Firepower /system # scope services
Firepower /system/services # create ntp-server 192.168.200.101
Firepower /system/services* # show configuration pending
  scope services
  + create ntp-server 192.168.200.101
  exit
Firepower /system/services* # commit-buffer
Firepower /system/services #

**Inline Help for the CLI**

At any time, you can enter the ? character to display the options available at the current state of the command syntax.

If you have not entered anything at the prompt, entering ? lists all available commands for the mode you are in. With a partially entered command, entering ? lists all keywords and arguments available at your current position in the command syntax.

**CLI Session Limits**

FXOS limits the number of CLI sessions that can be active at one time to 32 total sessions. This value is not configurable.
CHAPTER 3

Getting Started

- Task Flow, on page 9
- Initial Configuration, on page 9
- Accessing the FXOS CLI, on page 12

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 9).</td>
</tr>
<tr>
<td>Step 3</td>
<td>Set the Date and Time (see Setting the Date and Time, on page 57).</td>
</tr>
<tr>
<td>Step 4</td>
<td>Configure a DNS server (see Configuring DNS Servers, on page 97).</td>
</tr>
<tr>
<td>Step 5</td>
<td>Register your product license (see License Management for the ASA, on page 15).</td>
</tr>
<tr>
<td>Step 6</td>
<td>Configure users (see User Management, on page 25).</td>
</tr>
<tr>
<td>Step 7</td>
<td>Perform software updates as required (see Image Management, on page 43).</td>
</tr>
<tr>
<td>Step 8</td>
<td>Configure additional platform settings (see Platform Settings, on page 55).</td>
</tr>
<tr>
<td>Step 9</td>
<td>Configure interfaces (see Interface Management, on page 99).</td>
</tr>
<tr>
<td>Step 10</td>
<td>Create logical devices (see Logical Devices, on page 109).</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 1</th>
<th>Connect to the console port.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Power on the Firepower 9300 chassis.</td>
</tr>
</tbody>
</table>

You will see the power on self-test messages as the Firepower 9300 chassis boots.

<table>
<thead>
<tr>
<th>Step 3</th>
<th>When the unconfigured system boots, a setup wizard prompts you for the following information required to configure the system:</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

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**.

**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%958
Confirm the password for "admin": adminpassword%958
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 IP Address=192.168.10.10
Physical Switch Mgmt0 IP Netmask=255.255.255.0
Default Gateway=192.168.10.1
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 IP 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%652
Confirm the password for "admin": adminpassword%652
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 IPv6 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
IPv6 value=1
SSH Access Configured=yes
SSH IP Address=0.0.0.0
SSH IP Netmask=0.0.0.0
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:
Telnet is disabled by default. See Configuring Telnet, on page 62 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.

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, on page 15
- Prerequisites for Smart Software Licensing, on page 18
- Guidelines for Smart Software Licensing, on page 19
- Defaults for Smart Software Licensing, on page 19
- Configure Regular Smart Software Licensing, on page 19
- Configure a Smart License Satellite Server for the Firepower 9300 chassis, on page 21
- Monitoring Smart Software Licensing, on page 23
- History for Smart Software Licensing, on page 24

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.

Offline Management

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

Satellite Server

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

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

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

For more information, see the Smart Software Manager satellite installation and configuration guides on Smart Account Manager satellite.
Licenses and Devices Managed per Virtual Account

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

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

Evaluation License

The Firepower 9300 chassis supports two types of evaluation license:

- Chassis-level evaluation mode—Before the Firepower 9300 chassis registers with the Licensing Authority, it operates for 90 days (total usage) in evaluation mode. The ASA cannot request specific entitlements in this mode; only default entitlements are enabled. When this period ends, the Firepower 9300 chassis becomes out-of-compliance.

- Entitlement-based evaluation mode—After the Firepower 9300 chassis registers with the Licensing Authority, you can obtain time-based evaluation licenses that can be assigned to the ASA. In the ASA, you request entitlements as usual. When the time-based license expires, you need to either renew the time-based license or obtain a permanent license.

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

Smart Software Manager Communication

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

Device Registration and Tokens

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

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

Periodic Communication with the License Authority

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

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

### 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 or satellite server. There is no extra cost for secondary units.

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

scope monitoring
    scope callhome
    scope profile SLProf
    scope destination SLDest
    set address https://tools.cisco.com/its/service/oddce/services/DDCEService

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

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(Optional) Configure the HTTP Proxy, on page 19.</td>
</tr>
<tr>
<td>2</td>
<td>Register the Firepower Security Appliance with the License Authority, on page 20.</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

Step 1  Enable the HTTP proxy:

```
scope monitoring
scope callhome
set http-proxy-server-enable on
```

Example:
```
scope monitoring
  scope call-home
    set http-proxy-server-enable on
```

Step 2  Set the proxy URL:

```
set http-proxy-server-url url
```

where `url` is the http or https address of the proxy server.

Example:
```
set http-proxy-server-url https://10.1.1.1
```

Step 3  Set the port:

```
set http-proxy-server-port port
```

Example:
```
set http-proxy-server-port 443
```

Step 4  Commit the buffer:

```
commit-buffer
```

Register the Firepower Security Appliance with the License Authority

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

Procedure

Step 1  In the Smart Software Manager or the Smart Software Manager Satellite, request and copy a registration token for the virtual account to which you want to add this Firepower 9300 chassis.
For more information on how to request a registration token using the Smart Software Manager Satellite, see the Cisco Smart Software Manager Satellite User Guide (http://www.cisco.com/web/software/28628517/138897/Smart_Software_Manager_satellite_4.1.0_User_Guide.pdf).

Step 2  
Enter the registration token on the Firepower 9300 chassis:

```
scope license
register idtoken id-token
```

**Example:**
```
scope license
register idtoken ZGFmNWM5NjgtYmNjYS00ZWI3L
WE3NGItMWkGEwZjIxNGQ0LTE0NDYx%0AMDJzNT
V8N3R0dXM1Z0NjWkdpR214eFZmLdBOS9CvNvVEYyVKM1
q3R3vemRD%0AY29NQT0%3D%0A
```

Step 3  
To later unregister the device, enter:

```
scope license
deregister
```

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.

Step 4  
To renew the ID certificate and update the entitlements on all security modules, enter:

```
scope license
scope licdebug
renew
```

By default, the ID certificate is automatically renewed every 6 months, and the license entitlement is renewed every 30 days. You might want to manually renew the registration for either of these items if you have a limited window for Internet access, or if you make any licensing changes in the Smart Software Manager, for example.

## Configure a Smart License Satellite Server for the Firepower 9300 chassis

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

**Before you begin**
- Complete all prerequisites listed in the Prerequisites for Smart Software Licensing, on page 18.
- Download the Smart License Satellite OVA file from Cisco.com and install and configure it on a VMwareESXi server. For more information, see the Smart Software Manager satellite Install Guide.
If you do not already have a certificate chain, use the following procedures to request one:

- Create a key ring (Creating a Key Ring, on page 72).
- Create a certificate request for that key ring (Creating a Certificate Request for a Key Ring with Basic Options, on page 74).
- Send this certificate request to a trust anchor or Certificate Authority to obtain a certificate chain for your key ring.

For more information, see Certificates, Key Rings, and Trusted Points, on page 72.

### Procedure

**Step 1**
Set up the satellite server as the callhome destination:

```plaintext
scope monitoring
scope call-home
scope profile SLProfile
scope destination SLDest
set address https://ip_address/Transportgateway/services/DeviceRequestHandler
```

**Step 2**
Create a new trust point.

a) Enter security mode:

```plaintext
scope security
```

b) Create and name a trusted point:

```plaintext
create trustpoint trustpoint_name
```

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

```plaintext
set certchain certchain
```

For the `certchain` variable, use the certificate chain information obtained in the certificate generation prerequisite of this procedure.

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

d) Commit the configuration:

```plaintext
commit-buffer
```

**Example:**

```plaintext
firepower-chassis# scope security
firepower-chassis /security # create trustpoint tPoint10
firepower-chassis /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
```

Trustpoint Certificate Chain:

```plaintext
> -----BEGIN CERTIFICATE-----
```

---

Cisco Firepower 9300 FXOS CLI Configuration Guide, 1.1(3)
Step 3  Register the Firepower 9300 chassis with the License Authority (see Register the Firepower Security Appliance with the License Authority, on page 20). Note that you must request and copy the registration token from the Smart License Manager satellite.

Monitoring Smart Software Licensing

See the following commands for viewing license status:

- **show license all**
  
  Displays the state of Smart Software Licensing, Smart Agent version, UDI information, Smart Agent state, global compliance status, the entitlements status, licensing certificate information and schedule Smart Agent tasks.

- **show license status**

- **show license techsupport**
## 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 commands: deregister, register idtoken, renew, scope callhome, scope destination, scope licdebug, scope license, scope monitoring, scope profile, set address, set http-proxy-server-enable on, set http-proxy-server-url, set http-proxy-server-port, show license all, show license status, show license techsupport |
User Management

• User Accounts, on page 25
• Guidelines for Usernames, on page 26
• Guidelines for Passwords, on page 27
• Guidelines for Remote Authentication, on page 27
• User Roles, on page 30
• Password Profile for Locally Authenticated Users, on page 30
• Select the Default Authentication Service, on page 31
• Configuring the Session Timeout, on page 33
• Configuring the Role Policy for Remote Users, on page 33
• Enabling Password Strength Check for Locally Authenticated Users, on page 34
• Set the Maximum Number of Login Attempts, on page 35
• Configuring the Maximum Number of Password Changes for a Change Interval, on page 36
• Configuring a No Change Interval for Passwords, on page 37
• Configuring the Password History Count, on page 38
• Creating a Local User Account, on page 38
• Deleting a Local User Account, on page 41
• Activating or Deactivating a Local User Account, on page 41
• Clearing the Password History for a Locally Authenticated User, on page 42

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 27
• Configuring LDAP Providers, on page 85
• Configuring RADIUS Providers, on page 89
• Configuring TACACS+ Providers, on page 92

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 aaabb.
• 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>
</table>
| LDAP                    | Optional         | You can choose to do one of the following:  
  - Do not extend the LDAP schema and configure an existing, unused attribute that meets the requirements.  
  - Extend the LDAP schema and create a custom attribute with a unique name, such as CiscoAVPair. | The Cisco LDAP implementation requires a unicode type attribute.  
If you choose to create the CiscoAVPair custom attribute, use the following attribute ID:  
1.3.6.1.4.1.9.287247.1  
A sample OID is provided in the following section. |
<table>
<thead>
<tr>
<th>Authentication Provider</th>
<th>Custom Attribute</th>
<th>Schema Extension</th>
<th>Attribute ID Requirements</th>
</tr>
</thead>
</table>
| RADIUS                  | Optional         | You can choose to do one of the following:  
  • Do not extend the RADIUS schema and use an existing, unused attribute that meets the requirements.  
  • Extend the RADIUS schema and create a custom attribute with a unique name, such as cisco-avpair.  
|                         |                  | The vendor ID for the Cisco RADIUS implementation is 009 and the vendor ID for the attribute is 001.  
|                         |                  | The following syntax example shows how to specify multiples user roles and locales if you choose to create the cisco-avpair attribute:  
  `shell:roles="admin,aaa"`  
  `shell:locales="L1,abc"`.  
|                         |                  | Use a comma "," as the delimiter to separate multiple values. |
| TACAS                   | Required         | You must extend the schema and create a custom attribute with the name cisco-av-pair.  
|                         |                  | The cisco-av-pair name is the string that provides the attribute ID for the TACACS+ provider.  
|                         |                  | The following syntax example shows how to specify multiples user roles and locales when you create the cisco-av-pair attribute:  
  `cisco-av-pair=shell:roles="admin,aaa"`  
  `shell:locales="L1,abc"`. Using an asterisk (*) in the cisco-av-pair attribute syntax flags the locale as optional, preventing authentication failures for other Cisco devices that use the same authorization profile. Use a space as the delimiter to separate multiple values. |

**Sample OID for LDAP User Attribute**

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

```plaintext
CN=CiscoAVPair,CN=Schema,  
CN=Configuration,CN=X  
objectClass: top
```
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>
<tr>
<td>Password changes allowed within change interval</td>
<td>This option specifies the maximum number of times that passwords for locally authenticated users can be changed within a pre-defined interval. You can specify a change interval between 1 and 745 hours and a maximum number of password changes between 0 and 10. By default, a locally authenticated user is permitted a maximum of 2 password changes within a 48 hour interval.</td>
<td>For example, to allow a password to be changed a maximum of once within 24 hours after a locally authenticated user changes his or her password, set the following: • Change during interval to enable • Change count to 1 • Change interval to 24</td>
</tr>
</tbody>
</table>

Select the Default Authentication Service

Procedure

Step 1
Enter security mode:
Firepower-chassis # scope security

Step 2
Enter default authorization security mode:
Firepower-chassis /security # scope default-auth

Step 3
Specify the default authentication:
Firepower-chassis /security/default-auth # set realm auth-type
where auth-type is one of the following keywords:
• ldap—Specifies LDAP authentication
• local—Specifies local authentication
• none—Allows local users to log on without specifying a password
Step 4  (Optional) Specify the associated provider group, if any:

Firepower-chassis /security/default-auth # set auth-server-group auth-serv-group-name

Step 5  (Optional) Specify the maximum amount of time allowed between refresh requests for a user in this domain:

Firepower-chassis /security/default-auth # set refresh-period seconds

Specify an integer between 60 and 172800. The default is 600 seconds.

If this time limit is exceeded, FXOS considers the web session to be inactive, but it does not terminate the session.

Step 6  (Optional) Specify the maximum amount of time that can elapse after the last refresh request before FXOS considers a web session to have ended:

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

Specify an integer between 60 and 172800. The default is 7200 seconds.

**Note**  If you set two-factor authentication for a RADIUS or TACACS+ realm, consider increasing the session-refresh and session-timeout periods so that remote users do not have to reauthenticate too frequently.

Step 7  (Optional) Set the authentication method to two-factor authentication for the realm:

Firepower-chassis /security/default-auth # set use-2-factor yes

**Note**  Two-factor authentication applies only to the RADIUS and TACACS+ realms.

Step 8  Commit the transaction to the system configuration:

commit-buffer

---

**Example**

The following example sets the default authentication to RADIUS, the default authentication provider group to provider1, enables two-factor authentications, sets the refresh period to 300 seconds (5 minutes), the session timeout period to 540 seconds (9 minutes), and enables two-factor authentication. It then commits the transaction.

Firepower-chassis# scope security
Firepower-chassis /security # scope default-auth
Firepower-chassis /security/default-auth # set realm radius
Firepower-chassis /security/default-auth* # set auth-server-group provider1
Firepower-chassis /security/default-auth* # set use-2-factor yes
Firepower-chassis /security/default-auth* # set refresh-period 300
Firepower-chassis /security/default-auth* # set session-timeout 540
Firepower-chassis /security/default-auth* # commit-buffer
Firepower-chassis /security/default-auth #
Configuring the Session Timeout

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

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

Procedure

Step 1 Enter security mode:
Firepower-chassis # scope security

Step 2 Enter default authorization security mode:
Firepower-chassis/security # scope default-auth

Step 3 Set the idle timeout for HTTPS, SSH, and Telnet sessions:
Firepower-chassis/security/default-auth # set session-timeout seconds

Step 4 (Optional) Set the idle timeout for console sessions:
Firepower-chassis/security/default-auth # set con-session-timeout seconds

Step 5 (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:
Use of 2nd factor: No

Configuring the Role Policy for Remote Users

By default, read-only access is granted to all users logging in to Firepower Chassis Manager or the FXOS CLI from a remote server using the LDAP, RADIUS, or TACACS protocols. For security reasons, it might be desirable to restrict access to those users matching an established user role.

You can configure the role policy for remote users in the following ways:
assign-default-role

When a user attempts to log in and the remote authentication provider does not supply a user role with the authentication information, the user is allowed to log in with a read-only user role.

This is the default behavior.

no-login

When a user attempts to log in and the remote authentication provider does not supply a user role with the authentication information, access is denied.

Procedure

---

**Step 1**
Enter security mode:

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

**Step 2**
Specify whether user access to Firepower Chassis Manager and the FXOS CLI should be restricted based on user roles:

```bash
Firepower-chassis/security# set remote-user default-role {assign-default-role | no-login}
```

**Step 3**
Commit the transaction to the system configuration:

```bash
Firepower-chassis/security# commit-buffer
```

---

**Example**

The following example sets the role policy for remote users and commits the transaction:

```bash
Firepower-chassis# scope security
Firepower-chassis/security# set remote-user default-role no-login
Firepower-chassis/security*# commit-buffer
Firepower-chassis/security#
```

---

**Enabling Password Strength Check for Locally Authenticated Users**

If the password strength check is enabled, the Firepower eXtensible Operating System does not permit a user to choose a password that does not meet the guidelines for a strong password (see Guidelines for Passwords, on page 27).

**Procedure**

---

**Step 1**
Enter security mode:

```bash
Firepower-chassis# scope security
```
Step 2

Specify whether the password strength check is enabled or disabled:

Firepower-chassis /security # set enforce-strong-password {yes | no}

Example

The following example enables the password strength check:

Firepower-chassis# scope security
Firepower-chassis /security # set enforce-strong-password yes
Firepower-chassis /security* # commit-buffer
Firepower-chassis /security #

Set the Maximum Number of Login Attempts

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

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

Note

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

Procedure

Step 1

From the FXOS CLI, enter security mode:

scope system
scope security

Step 2

Set the maximum number of unsuccessful login attempts.

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:

set user-account-unlock-time

unlock_time

Step 4

Commit the configuration:
Configuring the Maximum Number of Password Changes for a Change Interval

Procedure

Step 1 Enter security mode:
Firepower-chassis # scope security
Step 2 Enter password profile security mode:
Firepower-chassis /security # scope password-profile
Step 3 Restrict the number of password changes a locally authenticated user can make within a given number of hours:
Firepower-chassis /security/password-profile # set change-during-interval enable
Step 4 Specify the maximum number of times a locally authenticated user can change his or her password during the Change Interval:
Firepower-chassis /security/password-profile # set change-count pass-change-num
This value can be anywhere from 0 to 10.
Step 5 Specify the maximum number of hours over which the number of password changes specified in the Change Count field are enforced:
Firepower-chassis /security/password-profile # set change-interval num-of-hours
This value can be anywhere from 1 to 745 hours.
For example, if this field is set to 48 and the Change Count field is set to 2, a locally authenticated user can make no more than 2 password changes within a 48 hour period.
Step 6 Commit the transaction to the system configuration:
Firepower-chassis /security/password-profile # commit-buffer

Example
The following example enables the change during interval option, sets the change count to 5, sets the change interval to 72 hours, and commits the transaction:
Firepower-chassis # scope security
Firepower-chassis /security # scope password-profile
Firepower-chassis /security/password-profile # set change-during-interval enable
Configuring a No Change Interval for Passwords

Procedure

Step 1  Enter security mode:
Firepower-chassis # scope security

Step 2  Enter password profile security mode:
Firepower-chassis /security # scope password-profile

Step 3  Disable the change during interval feature:
Firepower-chassis /security/password-profile # set change-during-interval disable

Step 4  Specify the minimum number of hours that a locally authenticated user must wait before changing a newly created password:
Firepower-chassis /security/password-profile # set no-change-interval min-num-hours
This value can be anywhere from 1 to 745 hours.
This interval is ignored if the Change During Interval property is not set to Disable.

Step 5  Commit the transaction to the system configuration:
Firepower-chassis /security/password-profile # commit-buffer

Example
The following example disables the change during interval option, sets the no change interval to 72 hours, and commits the transaction:
Firepower-chassis # scope security
Firepower-chassis /security # scope password-profile
Firepower-chassis /security/password-profile # set change-during-interval disable
Firepower-chassis /security/password-profile* # set no-change-interval 72
Firepower-chassis /security/password-profile* # commit-buffer
Firepower-chassis /security/password-profile #
Configuring the Password History Count

**Procedure**

**Step 1** Enter security mode:
Firepower-chassis# scope security

**Step 2** Enter password profile security mode:
Firepower-chassis/security# scope password-profile

**Step 3** Specify the number of unique passwords that a locally authenticated user must create before that user can reuse a previously used password:
Firepower-chassis/security/password-profile# set history-count num-of-passwords
This value can be anywhere from 0 to 15.
By default, the History Count field is set to 0, which disables the history count and allows users to reuse previously used passwords at any time.

**Step 4** Commit the transaction to the system configuration:
Firepower-chassis/security/password-profile# commit-buffer

**Example**
The following example configures the password history count and commits the transaction:

Firepower-chassis# scope security
Firepower-chassis/security# scope password-profile
Firepower-chassis/security/password-profile# set history-count 5
Firepower-chassis/security/password-profile*# commit-buffer

Creating a Local User Account

**Procedure**

**Step 1** Enter security mode:
Firepower-chassis# scope security

**Step 2** Create the user account:
Firepower-chassis/security# create local-user local-user-name
where \textit{local-user-name} is the account name to be 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 26).

After you create the user, the login ID cannot be changed. You must delete the user account and create a new one.

\textbf{Step 3} \hspace{1cm} Specify whether the local user account is enabled or disabled:

\texttt{Firepower-chassis/security/local-user # set account-status \{active\ inactive\}}

\textbf{Step 4} \hspace{1cm} Set the password for the user account:

\texttt{Firepower-chassis/security/local-user # set password}

Enter a password: \texttt{password}

Confirm the password: \texttt{password}

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 27).

\textbf{Step 5} \hspace{1cm} (Optional) Specify the first name of the user:

\texttt{Firepower-chassis/security/local-user # set firstname first-name}

\textbf{Step 6} \hspace{1cm} (Optional) Specify the last name of the user:

\texttt{Firepower-chassis/security/local-user # set lastname last-name}

\textbf{Step 7} \hspace{1cm} (Optional) Specify the date that the user account expires. The \textit{month} argument is the first three letters of the month name.

\texttt{Firepower-chassis/security/local-user # set expiration month day-of-month year}

\textbf{Note} \hspace{1cm} 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.

\textbf{Step 8} \hspace{1cm} (Optional) Specify the user e-mail address.

\texttt{Firepower-chassis/security/local-user # set email email-addr}

\textbf{Step 9} \hspace{1cm} (Optional) Specify the user phone number.

\texttt{Firepower-chassis/security/local-user # set phone phone-num}

\textbf{Step 10} \hspace{1cm} (Optional) Specify the SSH key used for passwordless access.

\texttt{Firepower-chassis/security/local-user # set sshkey ssh-key}

\textbf{Step 11} \hspace{1cm} All users are assigned the \textit{read-only} role by default and this role cannot be removed. For each additional role that you want to assign to the user:

\texttt{Firepower-chassis/security/local-user # create role role-name}

where \textit{role-name} is the role that represents the privileges you want to assign to the user account (see User Roles, on page 30).
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.

**Step 12**

To remove an assigned role from the user:

```
Firepower-chassis /security/local-user# delete role role-name
```

**Note**

All users are assigned the *read-only* role by default and this role cannot be removed.

**Step 13**

Commit the transaction.

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

---

**Example**

The following example creates the user account named kikipopo, enables the user account, sets the password to foo12345, assigns the admin user role, and commits the transaction:

```
Firepower-chassis# scope security
Firepower-chassis /security # create local-user kikipopo
Firepower-chassis /security/local-user* # set account-status active
Firepower-chassis /security/local-user* # set password
Enter a password:
Confirm the password:
Firepower-chassis /security/local-user* # create role admin
Firepower-chassis /security/local-user* # commit-buffer
```

The following example creates the user account named lincey, enables the user account, sets an OpenSSH key for passwordless access, assigns the aaa and operations user roles, and commits the transaction.

```
Firepower-chassis# scope security
Firepower-chassis /security # create local-user lincey
Firepower-chassis /security/local-user* # set account-status active
Firepower-chassis /security/local-user* # set sshkey "ssh-rsa AAAAB3NzaC1yc2EAAAABIA\nAAAIAwAAAEAEuosVQ2CmWB19/Slf30k1CWjyV31gdKm30GWU15iPw8\n3Jds4g+NFvNNm4cb4K iaqBBX/PQdmtl4QQSawc1j+k8f4VcOe1Bx1sK5luq5ls0b1V01EwcKEL/h5lrdbNII8y3SS9I/gSiB9ARlop9LDpD\nm8HPh2LQyH7EI1MF8=""
Firepower-chassis /security/local-user* # create role aaa
Firepower-chassis /security/local-user* # create role operations
Firepower-chassis /security/local-user* # commit-buffer
```

The following example creates the user account named jforlenz, enables the user account, sets a Secure SSH key for passwordless access, and commits the transaction.

```
Firepower-chassis# scope security
Firepower-chassis /security # create local-user jforlenz
Firepower-chassis /security/local-user* # set account-status active
Firepower-chassis /security/local-user* # set sshkey
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
User's SSH key:
> ---- BEGIN SSH2 PUBLIC KEY ----
> AAAAB3NzaC1yc2EAAAABIA\n> AAAIAwAAAEAEuosVQ2CmWB19/Slf30k1CWjyV31gdKm30GWU15iPw8
```

---
Deleting a Local User Account

Procedure

Step 1 Enter security mode:

Firepower-chassis# scope security

Step 2 Delete the local-user account:

Firepower-chassis /security # delete local-user local-user-name

Step 3 Commit the transaction to the system configuration:

Firepower-chassis /security # commit-buffer

Example

The following example deletes the foo user account and commits the transaction:

Firepower-chassis# scope security
Firepower-chassis /security # delete local-user foo
Firepower-chassis /security* # commit-buffer
Firepower-chassis /security #

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 Enter security mode:

Firepower-chassis# scope security

Step 2 Enter local-user security mode for the user you want to activate or deactivate:

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

Step 3 Specify whether the local user account is active or inactive:
Firepower-chassis /security/local-user # set account-status {active | inactive}

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

---

**Example**

The following example enables a local user account called accounting:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope local-user accounting
Firepower-chassis /security/local-user # set account-status active
```

---

**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 #
Image Management

• About Image Management, on page 43
• Downloading Images from Cisco.com, on page 44
• Downloading a Firepower eXtensible Operating System Software Image to the Firepower 9300 chassis, on page 44
• Verifying the Integrity of an Image, on page 45
• Upgrading the Firepower eXtensible Operating System Platform Bundle, on page 46
• Downloading a Logical Device Software Image to the Firepower 9300 chassis, on page 47
• Updating the Image Version for a Logical Device, on page 49
• Firmware Upgrade, on page 50

About Image Management

The Firepower 9300 chassis uses two basic types of images:

- Platform Bundle—The Firepower platform bundle is a collection of multiple independent images that operate on the Firepower Supervisor and Firepower security module/engine. The platform bundle is a Firepower eXtensible Operating System software package.

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

Note

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.

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

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

Before you begin
You must have a Cisco.com account.

Procedure

Step 1
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.

Downloading a Firepower eXtensible Operating System Software Image to the Firepower 9300 chassis

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

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

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

Procedure

Step 1
Enter firmware mode:
Firepower-chassis # scope firmware

Step 2
Download the FXOS software image:
Firepower-chassis /firmware # download image URL
Specify the URL for the file being imported using one of the following syntax:

- ftp://username@hostname/path/image_name
- scp://username@hostname/path/image_name
- sftp://username@hostname/path/image_name
- tftp://hostname:port-num/path/image_name
Step 3  To monitor the download process:
Firepower-chassis /firmware # show package image_name detail

---

**Example**

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image scp://user@192.168.1.1/images/fxos-k9.1.1.119.SPA
Firepower-chassis /firmware # show package fxos-k9.1.1.119.SPA detail
```

Download task:
- File Name: fxos-k9.1.1.119.SPA
- Protocol: scp
- Server: 192.168.1.1
- Userid:
- Path:
- Downloaded Image Size (KB): 5120
- State: Downloading


---

**Verifying the Integrity of an Image**

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

**Procedure**

**Step 1**  Connect to the FXOS CLI (see *Accessing the FXOS CLI, on page 12*).
**Step 2**  Enter firmware mode:
Firepower-chassis# scope firmware

**Step 3**  List images:
Firepower-chassis /firmware # show package

**Step 4**  Verify the image:
Firepower-chassis /firmware # verify platform-pack version version_number

*version_number* is the version number of the FXOS platform bundle you are verifying--for example, 1.1(2.51).

**Step 5**  The system will warn you that verification could take several minutes.
Enter **yes** to confirm that you want to proceed with verification.

**Step 6**  To check the status of the image verification:
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 44) and then download that image to the Firepower 9300 chassis (see Downloading a Logical Device Software Image to the Firepower 9300 chassis, on page 47).

Procedure

Step 1  Connect to the FXOS CLI (see Accessing the FXOS CLI, on page 12).
Step 2  Enter firmware mode:
Firepower-chassis# scope firmware
Step 3  Enter auto-install mode:
Firepower-chassis /firmware # scope auto-install
Step 4  Install the FXOS platform bundle:
Firepower-chassis /firmware/auto-install # install platform platform-vers version_number
version_number is the version number of the FXOS platform bundle you are installing--for example, 1.1(2.51).
Step 5  The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.
Enter yes to confirm that you want to proceed with verification.
Step 6  Enter yes to confirm that you want to proceed with installation, or enter no to cancel the installation.
The Firepower eXtensible Operating System unpacks the bundle and upgrades/reloads the components.
Step 7  To monitor the upgrade process:
a) Enter scope firmware.
b) Enter scope auto-install.
c) Enter show fsm status expand.
Downloading a Logical Device Software Image to the Firepower 9300 chassis

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

Before you begin
Collect the following information that you will need to import a configuration file:
- IP address and authentication credentials for the server from which you are copying the image
- Fully qualified name of the software image file

Procedure

Step 1  Enter Security Services mode:
Firepower-chassis # scope ssa

Step 2  Enter Application Software mode:
Firepower-chassis /ssa # scope app-software

Step 3  Download the logical device software image:
Firepower-chassis /ssa/app-software # download image URL
Specify the URL for the file being imported using one of the following syntax:
- ftp://username@hostname/path
- scp://username@hostname/path
- sftp://username@hostname/path
- tftp://hostname:port-num/path

Step 4  To monitor the download process:
Firepower-chassis /ssa/app-software # show download-task

Step 5  To view the downloaded applications:
Firepower-chassis /ssa/app-software # up
Firepower-chassis /ssa # show app

Step 6  To view details for a specific application:
Firepower-chassis /ssa # scope app application_type image_version
Firepower-chassis /ssa/app # show expand

Example

The following example copies an image using the SCP protocol:

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

Downloads for Application Software:
<table>
<thead>
<tr>
<th>File Name</th>
<th>Protocol</th>
<th>Server</th>
<th>Userid</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>cisco-asa.9.4.1.65.csp</td>
<td>Scp</td>
<td>192.168.1.1</td>
<td>user</td>
<td>Downloaded</td>
</tr>
</tbody>
</table>
```

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:

```
<table>
<thead>
<tr>
<th>Name</th>
<th>Version</th>
<th>Description</th>
<th>Author</th>
<th>Deploy Type</th>
<th>CSP Type</th>
<th>Is Default App</th>
</tr>
</thead>
<tbody>
<tr>
<td>asa</td>
<td>9.4.1.41</td>
<td>N/A</td>
<td>N/A</td>
<td>Native</td>
<td>Application</td>
<td>No</td>
</tr>
<tr>
<td>asa</td>
<td>9.4.1.65</td>
<td>N/A</td>
<td>N/A</td>
<td>Native</td>
<td>Application</td>
<td>Yes</td>
</tr>
</tbody>
</table>
```

Firepower-chassis /ssa # scope app asa 9.4.1.65

Firepower-chassis /ssa/app # show expand

Application:

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

App Attribute Key for the Application:
<table>
<thead>
<tr>
<th>App Attribute Key Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster-role</td>
</tr>
<tr>
<td>mgmt-ip</td>
</tr>
<tr>
<td>mgmt-url</td>
</tr>
</tbody>
</table>

Net Mgmt Bootstrap Key for the Application:
```
<table>
<thead>
<tr>
<th>Bootstrap Key Data Type</th>
<th>Key Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PASSWORD</td>
<td></td>
</tr>
</tbody>
</table>
```

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

Port Type: Mgmt
Max Ports: 1
Min Ports: 1
```
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 44) and then download that image to the Firepower 9300 chassis (see Downloading a Logical Device Software Image to the Firepower 9300 chassis, on page 47).

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**
Enter Security Services mode:
Firepower-chassis # scope ssa

**Step 2**
Set the scope to the security module you are updating:
Firepower-chassis /ssa # scope slot slot_number
**Firmware Upgrade**

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

**Procedure**

**Step 1**
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:
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
```

<table>
<thead>
<tr>
<th>Name</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>fxos-k9-fpr9k-firmware.1.0.10.SPA</td>
<td>1.0.10</td>
</tr>
</tbody>
</table>

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 55
- Setting the Date and Time, on page 57
- Configuring SSH, on page 62
- Configuring Telnet, on page 62
- Configuring SNMP, on page 63
- Configuring HTTPS, on page 71
- Configuring AAA, on page 83
- Configuring Syslog, on page 94
- Configuring DNS Servers, on page 97

Changing the Management IP Address

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

Procedure

Step 1
Connect to the FXOS CLI (see Accessing the FXOS CLI, on page 12).

Step 2
To configure an IPv4 management IP address:

a) Set the scope for fabric-interconnect a:

    Firepower-chassis# scope fabric-interconnect a

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

    Firepower-chassis /fabric-interconnect # show

c) Enter the following command to configure a new management IP address and gateway:
Step 3
To configure an IPv6 management IP address:

a) Set the scope for fabric-interconnect a:

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

b) Set the scope for management IPv6 configuration:

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

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

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

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

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

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 :: :: 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
```

The following example configures an IPv6 management interface and gateway:

```
Firepower-chassis# scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # scope ipv6-config
Firepower-chassis /fabric-interconnect/ipv6-config # show ipv6-if
```
Management IPv6 Interface:
<table>
<thead>
<tr>
<th>IPv6 Address</th>
<th>Prefix</th>
<th>IPv6 Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001::8998</td>
<td>64</td>
<td>2001::1</td>
</tr>
</tbody>
</table>

Firepower-chassis /fabric-interconnect/ipv6-config # set out-of-band ipv6 2001::8999
ipv6-prefix 64 ipv6-gw 2001::1
Firepower-chassis /fabric-interconnect/ipv6-config* # commit-buffer
Firepower-chassis /fabric-interconnect/ipv6-config #

## Setting the Date and Time

Use the CLI commands described below 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**

Enter system mode:

Firepower-chassis# scope system

**Step 2**

Enter system services mode:

Firepower-chassis /system # scope services

**Step 3**

Set the time zone:

Firepower-chassis /system/services # set timezone

At this point, you are prompted to enter a number corresponding to your continent, country, and time zone region. Enter the appropriate information at each prompt.

When you have finished specifying the location information, you are prompted to confirm that the correct time zone information is being set. Enter 1 (yes) to confirm, or 2 (no) to cancel the operation.

**Step 4**

To view the configured time zone:

Firepower-chassis /system/services # top

Firepower-chassis# show timezone

### Example

The following example configures the time zone to the Pacific time zone region, commits the transaction, and displays the configured time zone:
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # set timezone

Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa 4) Arctic Ocean 7) Australia 10) Pacific Ocean
2) Americas 5) Asia 8) Europe
3) Antarctica 6) Atlantic Ocean 9) Indian Ocean

Please select a country.
1) Anguilla 28) Haiti
2) Antigua & Barbuda 29) Honduras
3) Argentina 30) Jamaica
4) Aruba 31) Martinique
5) Bahamas 32) Mexico
6) Barbados 33) Montserrat
7) Belize 34) Nicaragua
8) Bolivia 35) Panama
9) Brazil 36) Paraguay
10) Canada 37) Peru
11) Caribbean Netherlands 38) Puerto Rico
12) Cayman Islands 39) St Barthelemy
13) Chile 40) St Kitts & Nevis
14) Colombia 41) St Lucia
15) Costa Rica 42) St Maarten (Dutch part)
16) Cuba 43) St Martin (French part)
17) Curacao 44) St Pierre & Miquelon
18) Dominica 45) St Vincent
19) Dominican Republic 46) Suriname
20) Ecuador 47) Trinidad & Tobago
21) El Salvador 48) Turks & Caicos Is
22) French Guiana 49) United States
23) Greenland 50) Uruguay
24) Grenada 51) Venezuela
25) Guadeloupe 52) Virgin Islands (UK)
26) Guatemala 53) Virgin Islands (US)
27) Guyana

Please select one of the following time zone regions.
1) Eastern Time
2) Eastern Time - Michigan - most locations
3) Eastern Time - Kentucky - Louisville area
4) Eastern Time - Kentucky - Wayne County
5) Eastern Time - Indiana - most locations
6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
7) Eastern Time - Indiana - Pulaski County
8) Eastern Time - Indiana - Crawford County
9) Eastern Time - Indiana - Pike County
10) Eastern Time - Indiana - Switzerland County
11) Central Time
12) Central Time - Indiana - Perry County
13) Central Time - Indiana - Starke County
14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
15) Central Time - North Dakota - Oliver County
16) Central Time - North Dakota - Morton County (except Mandan area)
17) Central Time - North Dakota - Mercer County
18) Mountain Time
19) Mountain Time - south Idaho & east Oregon
20) Mountain Standard Time - Arizona (except Navajo)
21) Pacific Time
22) Pacific Standard Time - Annette Island, Alaska
23) Alaska Time
24) Alaska Time - Alaska panhandle
25) Alaska Time - southeast Alaska panhandle
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 Enter system mode:
Firepower-chassis# scope system

Step 2 Enter system services mode:
Firepower-chassis /system # scope services

Step 3 Configure the system to use the NTP server with the specified hostname, IPv4, or IPv6 address:
Firepower-chassis /system/services # create ntp-server /hostname | ip-addr | ip6-addr

Step 4 Commit the transaction to the system configuration:
Firepower-chassis /system/services # commit-buffer

Step 5 To view the synchronization status for all configured NTP servers:
Firepower-chassis /system/services # show ntp-server

Step 6 To view the synchronization status for a specific NTP server:
Firepower-chassis /system/services # scope ntp-server /hostname | ip-addr | ip6-addr
Example

The following example configures an NTP server with the IP address 192.168.200.101 and commits the transaction:

```plaintext
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # create ntp-server 192.168.200.101
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

The following example configures an NTP server with the IPv6 address 4001::6 and commits the transaction:

```plaintext
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # create ntp-server 4001::6
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

Deleting an NTP Server

Procedure

1. **Enter system mode:**
   Firepower-chassis# scope system

2. **Enter system services mode:**
   Firepower-chassis /system # scope services

3. **Delete the NTP server with the specified hostname, IPv4, or IPv6 address:**
   Firepower-chassis /system/services # delete ntp-server {hostname | ip-addr | ip6-addr}

4. **Commit the transaction to the system configuration:**
   Firepower-chassis /system/services # commit-buffer

Example

The following example deletes the NTP server with the IP address 192.168.200.101 and commits the transaction:

```plaintext
Firepower-chassis# scope system
Firepower-chassis /system # scope services
```
The following example deletes the NTP server with the IPv6 address 4001::6 and commits the transaction:

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # delete ntp-server 4001::6
Firepower-chassis /system/services* # commit-buffer
```

---

### Setting the Date and Time Manually

This section describes how to set the date and time manually on the Firepower chassis. System clock modifications take effect immediately.

---

**Note**

If the system clock is currently being synchronized with an NTP server, you will not be able to set the date and time manually.

---

**Procedure**

**Step 1**

Enter system mode:

```
Firepower-chassis# scope system
```

**Step 2**

Enter system services mode:

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

**Step 3**

Configure the system clock:

```
Firepower-chassis /system/services # set clock month day year hour min sec
```

For month, use the first three digits of the month. Hours must be entered using the 24-hour format, where 7 pm would be entered as 19.

System clock modifications take effect immediately. You do not need to commit the buffer.

---

**Example**

The following example configures the system clock:

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # set clock jun 24 2015 15 27 00
Firepower-chassis /system/services #
```
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**
Enter system mode:
Firepower-chassis # scope system

**Step 2**
Enter system services mode:
Firepower-chassis /system # scope services

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

- To allow SSH access to the Firepower chassis, enter the following command:
  Firepower-chassis /system/services # enable ssh-server
- To disallow SSH access to the Firepower chassis, enter the following command:
  Firepower-chassis /system/services # disable ssh-server

**Step 4**
Commit the transaction to the system configuration:
Firepower /system/services # commit-buffer

**Example**
The following example enables SSH access to the Firepower chassis and commits the transaction:

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

Configuring Telnet

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

**Note**
Telnet configuration is currently only available using the CLI.
Procedure

Step 1
Enter system mode:
Firepower-chassis # scope system

Step 2
Enter system services mode:
Firepower-chassis /system # scope services

Step 3
To configure Telnet access to the Firepower chassis, do one of the following:
- To allow Telnet access to the Firepower chassis, enter the following command:
  Firepower-chassis /system/services # enable telnet-server
- To disallow Telnet access to the Firepower chassis, enter the following command:
  Firepower-chassis /system/services # disable telnet-server

Step 4
Commit the transaction to the system configuration:
Firepower /system/services # commit-buffer

Example
The following example enables Telnet and commits the transaction:
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /services # enable telnet-server
Firepower-chassis /services* # commit-buffer
Firepower-chassis /services #

Configuring SNMP

This section describes how 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
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

Step 1  Enter monitoring mode:
Firepower-chassis# scope monitoring

Step 2  Enable SNMP:
Firepower-chassis /monitoring # enable snmp

Step 3  Enter snmp community mode:
Firepower-chassis /monitoring # set snmp community
After you enter the set snmp community command, you are prompted to enter the SNMP community.

Step 4  Specify the SNMP community. Use the community name as a password. The community name can be any alphanumeric string up to 32 characters.
Firepower-chassis /monitoring # Enter a snmp community: community-name

Step 5  Specify the system contact person responsible for SNMP. The system contact name can be any alphanumeric string up to 255 characters, such as an email address or name and telephone number.
Firepower-chassis /monitoring # set snmp syscontact system-contact-name

Step 6  Specify the location of the host on which the SNMP agent (server) runs. The system location name can be any alphanumeric string up to 512 characters.
Firepower-chassis /monitoring # set snmp syslocation system-location-name

Step 7  Commit the transaction to the system configuration:
Example
The following example enables SNMP, configures an SNMP community named SnmpCommSystem2, configures a system contact named contactperson, configures a contact location named systemlocation, and commits the transaction:

```
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # enable snmp
Firepower-chassis /monitoring* # set snmp community
Enter a snmp community: SnmpCommSystem2
Firepower-chassis /monitoring* # set snmp syscontact contactperson1
Firepower-chassis /monitoring* # set snmp syslocation systemlocation
Firepower-chassis /monitoring* # commit-buffer
```

What to do next
Create SNMP traps and users.

Creating an SNMP Trap

Procedure

1. **Step 1** Enter monitoring mode:
   ```
   Firepower-chassis# scope monitoring
   ```

2. **Step 2** Enable SNMP:
   ```
   Firepower-chassis /monitoring # enable snmp
   ```

3. **Step 3** Create an SNMP trap with the specified host name, IPv4 address, or IPv6 address.
   ```
   Firepower-chassis /monitoring # create snmp-trap {hostname | ip-addr | ip6-addr}
   ```

4. **Step 4** Specify the SNMP community name to be used for the SNMP trap:
   ```
   Firepower-chassis /monitoring/snmp-trap # set community community-name
   ```

5. **Step 5** Specify the port to be used for the SNMP trap:
   ```
   Firepower-chassis /monitoring/snmp-trap # set port port-num
   ```

6. **Step 6** Specify the SNMP version and model used for the trap:
   ```
   Firepower-chassis /monitoring/snmp-trap # set version {v1 | v2c | v3}
   ```

7. **Step 7** (Optional) Specify the type of trap to send.
   ```
   Firepower-chassis /monitoring/snmp-trap # set notificationtype {traps | informs}
   ```
   This can be:
Creating an SNMP Trap

- traps if you select v2c or v3 for the version.
- informs if you select v2c for the version.

Note: An inform notification can be sent only if you select v2c for the version.

**Step 8** (Optional) If you select v3 for the version, specify the privilege associated with the trap:

Firepower-chassis /monitoring/snmp-trap# set v3privilege \{auth | noauth | priv\}

This can be:

- **auth**—Authentication but no encryption
- **noauth**—No authentication or encryption
- **priv**—Authentication and encryption

**Step 9** Commit the transaction to the system configuration:

Firepower-chassis /monitoring/snmp-trap# commit-buffer

---

**Example**

The following example enables SNMP, creates an SNMP trap using an IPv4 address, specifies that the trap will use the SnmpCommSystem2 community on port 2, sets the version to v3, sets the notification type to traps, sets the v3 privilege to priv, and commits the transaction:

```
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # enable snmp
Firepower-chassis /monitoring* # create snmp-trap 192.168.100.112
Firepower-chassis /monitoring/snmp-trap* # set community SnmpCommSystem2
Firepower-chassis /monitoring/snmp-trap* # set port 2
Firepower-chassis /monitoring/snmp-trap* # set version v3
Firepower-chassis /monitoring/snmp-trap* # set notificationtype traps
Firepower-chassis /monitoring/snmp-trap* # set v3privilege priv
Firepower-chassis /monitoring/snmp-trap* # commit-buffer
```

The following example enables SNMP, creates an SNMP trap using an IPv6 address, specifies that the trap will use the SnmpCommSystem3 community on port 2, sets the version to v3, sets the notification type to traps, sets the v3 privilege to priv, and commits the transaction:

```
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # enable snmp
Firepower-chassis /monitoring* # create snmp-trap 2001::1
Firepower-chassis /monitoring/snmp-trap* # set community SnmpCommSystem3
Firepower-chassis /monitoring/snmp-trap* # set port 2
Firepower-chassis /monitoring/snmp-trap* # set version v3
Firepower-chassis /monitoring/snmp-trap* # set notificationtype traps
Firepower-chassis /monitoring/snmp-trap* # set v3privilege priv
Firepower-chassis /monitoring/snmp-trap* # commit-buffer
```

---
Deleting an SNMP Trap

**Procedure**

**Step 1**
Enter monitoring mode:
```
Firepower-chassis# scope monitoring
```

**Step 2**
Delete the SNMP trap with the specified hostname or IP address:
```
Firepower-chassis /monitoring# delete snmp-trap {hostname | ip-addr}
```

**Step 3**
Commit the transaction to the system configuration:
```
Firepower-chassis /monitoring# commit-buffer
```

**Example**
The following example deletes the SNMP trap at IP address 192.168.100.112 and commits the transaction:
```
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring# delete snmp-trap 192.168.100.112
Firepower-chassis /monitoring* # commit-buffer
Firepower-chassis /monitoring#
```

Creating an SNMPv3 User

**Procedure**

**Step 1**
Enter monitoring mode:
```
Firepower-chassis# scope monitoring
```

**Step 2**
Enable SNMP:
```
Firepower-chassis /monitoring# enable snmp
```

**Step 3**
Create the specified SNMPv3 user:
```
Firepower-chassis /monitoring# create snmp-user user-name
```

After you enter the `create snmp-user` command, you are prompted to enter the password.

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:
  ```
  ~`!@#$%^&*()-{}[]\|:;"'<,./
  ```
Creating an SNMPv3 User

- 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.

Step 4 Enable or disable the use of AES-128 encryption:

Firepower-chassis /monitoring/snmp-user # set aes-128 {no | yes}

By default, AES-128 encryption is disabled.

Step 5 Specify the user privacy password:

Firepower-chassis /monitoring/snmp-user # set priv-password

After you enter the set priv-password command, you are prompted to enter and confirm the privacy password. 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.

Step 6 Commit the transaction to the system configuration:

Firepower-chassis /monitoring/snmp-user # commit-buffer

Example

The following example enables SNMP, creates an SNMPv3 user named snmp-user14, enables AES-128 encryption, sets the password and privacy password, and commits the transaction:
Deleting an SNMPv3 User

Procedure

Step 1  Enter monitoring mode:
Firepower-chassis# scope monitoring

Step 2  Delete the specified SNMPv3 user:
Firepower-chassis /monitoring # delete snmp-user user-name

Step 3  Commit the transaction to the system configuration:
Firepower-chassis /monitoring # commit-buffer

Example
The following example deletes the SNMPv3 user named snmp-user14 and commits the transaction:
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # delete snmp-user snmp-user14
Firepower-chassis /monitoring* # commit-buffer

Configuring HTTPS

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

Note
You can change the HTTPS port using Firepower Chassis Manager or the FXOS CLI. All other HTTPS configuration can only be done using the FXOS CLI.
Certificates, Key Rings, and Trusted Points

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

Encryption Keys and Key Rings

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

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

Certificates

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

Trusted Points

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

Important

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

Creating a Key Ring

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

Procedure

Step 1

Enter security mode:

Firepower-chassis # scope security
Step 2 Create and name the key ring:
Firepower-chassis# create keyring keyring-name

Step 3 Set the SSL key length in bits:
Firepower-chassis# set modulus {mod1024 | mod1536 | mod2048 | mod512}

Step 4 Commit the transaction:
Firepower-chassis# commit-buffer

---

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

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

What to do next
Create a certificate request for this key ring.

Regenerating the Default Key Ring

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

Procedure

Step 1 Enter security mode:
Firepower-chassis# scope security

Step 2 Enter key ring security mode for the default key ring:
Firepower-chassis /security # scope keyring default

Step 3 Regenerate the default key ring:
Firepower-chassis /security/keyring# set regenerate yes

Step 4 Commit the transaction:
Firepower-chassis# commit-buffer
Example
The following example regenerates the default key ring:

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

Creating a Certificate Request for a Key Ring

Creating a Certificate Request for a Key Ring with Basic Options

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 1 | Enter security mode:  
Firepower-chassis # scope security |
| Step 2 | Enter configuration mode for the key ring:  
Firepower-chassis /security # scope keyring keyring-name |
| Step 3 | Create a certificate request using the IPv4 or IPv6 address specified, or the name of the fabric interconnect. You are prompted to enter a password for the certificate request.  
Firepower-chassis /security/keyring # create certreq {ip [ipv4-addr | ipv6-v6] |subject-name name} |
| Step 4 | Commit the transaction:  
Firepower-chassis /security/keyring/certreq # commit-buffer |
| Step 5 | Display the certificate request, which you can copy and send to a trust anchor or certificate authority:  
Firepower-chassis /security/keyring # show certreq |

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

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # create certreq ip 192.168.200.123 subject-name sjc04
Certificate request password:  
Confirm certificate request password:  
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request e-mail name:
```
Certificate request country name:
State, province or county (full name):
Locality (eg, city):
Organization name (eg, company):
Organization Unit name (eg, section):
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8gMZQ0UGqILKFXQQc2c8B/vW2rnRF80PhKbhgLAIYZIF
JqcYE55Y11+vgohLBt45sOGC8m4RTLJWHO4SwccAUQXQ5znqf45YtX1WsyiwUNV4
0re/zgTk/Wcd56rOObvWR2dztzu2pgA14ad761zLxt29K7R8mzj6CAUVAgMBAAGg
LTAkBqkhkiG9wUBCQ4xHjAcMBoGAIUDEQE/8QQMA6CBnNhbWMwN1cECsE1XJAN
BgkqhkiG9w0BAQQFAAOBgC8xN0qUHYGFzQ56RwQueLTNFnrndqUwuZHS03Teq
nhyu4satpypQ7fV9vikZ+spvc6x5PWIcTWgHhh8BiO/0OKu6kwfIOSSED1Av
TTYvU+BE9OF1FrB1A718S+V8ndxIHejiQGx1DmqoN+odCNPc5kJjO01T09H
BA==
-----END CERTIFICATE REQUEST-----

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 # 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:
Creating a Certificate Request for a Key Ring with Advanced Options

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

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

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

**Step 9** Specify the organization requesting the certificate:

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

**Step 10** Specify the organizational unit:

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

**Step 11** Specify an optional password for the certificate request:

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

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

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

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

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

**Step 14** Commit the transaction:

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

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

Firepower-chassis /security/keyring # show certreq

---

**Example**

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

Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # create certreq
Firepower-chassis /security/keyring/certreq* # set ip 192.168.200.123
Firepower-chassis /security/keyring/certreq* # set subject-name sjc04
Firepower-chassis /security/keyring/certreq* # set country US
Firepower-chassis /security/keyring/certreq* # set dns bg1-samc-15A
Firepower-chassis /security/keyring/certreq* # set email test@cisco.com
Firepower-chassis /security/keyring/certreq* # set locality new york city
Firepower-chassis /security/keyring/certreq* # set org-name "Cisco Systems"
Firepower-chassis /security/keyring/certreq* # set org-unit-name Testing
Firepower-chassis /security/keyring/certreq* # set state new york
Firepower-chassis /security/keyring/certreq* # commit-buffer
Firepower-chassis /security/keyring/certreq* # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request e-mail name: test@cisco.com
Certificate request country name: US
State, province or county (full name): New York
Locality name (eg, city): new york city
Organization name (eg, company): Cisco
Organization Unit name (eg, section): Testing
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
qYAMIGJJAoGBALpKn1t8gME4UgILKFXQCc2c8b/vW2rNF08PPhKhghhLA1YZ1F
JqYEGSY11+vyohLBt4sOC8m4RTLJWHO4SwccAUUXQ5Zngf45YtX1WyylwNWF4
0re/zytk/WD56RfOBwWR2Dtszu2pGA14sd761zLxth29K7R8mzj6CAUVAgMBAAgq
LTA9BkgkhkI9w08BCQ4xHJAcMBoGA1UDQEjEB/wQQA6CBnNhWMMwNiECAEeIXJAN
BkgkhkI9w0BAQFAQOBOgCswxNOuYYFQOW56RwQueLTNfrndeUwuZHU03Teq
nhsyu4satpy1PqVY9iKZ+spvc6x5FW1cTWgHN8BiOb/U0Rug8kwfIGsED1Av
TTYvUF+BZ9F1PbRIA718S+V8ndXr1HejiQGx1DNqON+ocCXPc5kjoXD0LT09H
BA==
-----END CERTIFICATE REQUEST-----

Firepower-chassis /security/keyring/certreq #

What to do next

• Copy the text of the certificate request, including the BEGIN and END lines, and save it in a file. Send the file with the certificate request to a trust anchor or certificate authority to obtain a certificate for the key ring.

• Create a trusted point and set the certificate chain for the certificate of trust received from the trust anchor.

Creating a Trusted Point

Procedure

Step 1
Enter security mode:
Firepower-chassis # scope security

Step 2
Create a trusted point:
Firepower-chassis /security # create trustpoint name

Step 3
Specify certificate information for this trusted point:
Firepower-chassis /security/trustpoint # set certchain [certchain]

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

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

Step 4
Commit the transaction:
Firepower-chassis /security/trustpoint # commit-buffer
Example

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

```
Firepower-chassis# scope security
Firepower-chassis /security # create trustpoint tPoint10
Firepower-chassis /security/trustpoint* # set cert
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
> -----BEGIN CERTIFICATE-----
> MIIDMDCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJVUzEL
> BwIBattaBIGaECCAdwQgZ8wDQYJKoZIhvcNAQEBBQADSwIBADAdBgNVHQ4MBDAETAQ
> 5gIEGAgMBAAIGNj01bnR5c3RldGEgY29udGluZy5wczAuMCgGCCsGAQUFBwMBBggrG
> A1UDBAIBBggpGq0BAQEEgYwDQYJKoZIhvcNAQEFBQADggYEAE61CaJo3aVMhzCl90306
> MG51zq1zXcz75+VFj2I6r9asckCld3mkoVx5zjU
> Ptt5CVqNgNLdvDPSxxtzysOhtysOhmpH9+CLv8Fbui1CDYfaalt1WvfeheksV0j6
> 421ido3n04MIGeBvWNHSMExgZ2AFLiMjtscMY²f²+3yb42
> 1ido3n04Okldjd80MOqweCYDVQOEwJUVlzELMakGAIUEBMCQ0ExFADASgNVBAC7
> C1nhbnnIeNxEEYhmjRweqWYDVQOEkxJ0d9W2tSeXZ0NWZlIeUUy4KFADASgNV
> BA1TC0Vz2UuZWYWm5nMq8WqDyDQOxEE20XNRQ0CaAQwDAyDVR0TBAlAwEi
> //zANBkgkqhXGw90BQQFAdgqAhWraXN6B4g6iLenr+fptHv+WWhB5fKgQgXc
> wR4yiO4z42/9Jtjenh751CkMw51az8copPEOmcYynhfs5C6vassenn1ddkYt4
> PR0VxGcDc0WhuiozBolesmmjBbedUCwQgdFDFHfIDIZKw5+N3x/kfa2EHU6id1avt
> 4YL5Jg==
> -----END CERTIFICATE-----
> ENDOFBUF
```

What to do next

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

Importing a Certificate into a Key Ring

Before you begin

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

Procedure

**Step 1**
Enter security mode:

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

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

```
Firepower-chassis /security # scope keyring keyring-name
```
Step 3 Specify the trusted point for the trust anchor or certificate authority from which the key ring certificate was obtained:

Firepower-chassis /security/keyring # set trustpoint name

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

Firepower-chassis /security/keyring # set cert

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

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

Step 5 Commit the transaction:

Firepower-chassis /security/keyring # commit-buffer

---

**Example**

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

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # set trustpoint tPoint10
Firepower-chassis /security/keyring* # set cert

Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.

Keyring certificate:

> -----BEGIN CERTIFICATE-----
> MIIB/zCCAwCAQAwg2kxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGtcGxlIIE1uYy4xExZARBgNVBAAsT
> AoGBAMw4nTepNIDhVzboj7Z2Je4xAG56zmSMRMeOGHemdh66u2/XAoLox7YCCu1D
> 7gA1vyyC3gf/K6CjQtoflvr3mc/eAehuK3/SINv7wd6Vv2pB662pXgD4VBNKOND1
> G6kbPervy1JbG4MD2dx2+H8EHi3Mtd2rzQvFxEKJSEhA9GbqETb1F5wZVNAgMBAGAgJTAjBkgq
> hkiG9wBQcxiHqMSQ6bjaGFVv2ZugvGaGFVz3dvcwQDQYJRoZIHvceNAQEBQgADF
> g1EAG61CaJoVaM1hzCl90306Mg51zq1zXcoz75+VFj2I6rH9asckCld3mkOVx5gJU
> Pt5VCqNgNLDvbDPsxXeytsOHqHmp9+CLv8FDyl1CDYfuLtv1WfhevskV0j6
> m3kR6+10G7m0809mGqaw8z/hy1/L431fIP1Nh503oha4="
> -----END CERTIFICATE-----
> END OF BUF

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](http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite).

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

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

**Step 8** Commit the transaction to the system configuration:
```
Firepower-chassis /system/services # commit-buffer
```
Example

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

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

Changing the HTTPS Port

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

Procedure

---

**Step 1**
Enter system mode:

```
Firepower-chassis # scope system
```

**Step 2**
Enter system services mode:

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

**Step 3**
Specify the port to use for HTTPS connections:

```
Firepower-chassis /system/services # set https port port-number
```

Specify an integer between 1 and 65535 for `port-number`. HTTPS is enabled on port 443 by default.

**Step 4**
Commit the transaction to the system configuration:

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

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.

---

Example

The following example sets the HTTPS port number to 443 and commits the transaction:

```
```
Deleting a Key Ring

**Procedure**

**Step 1**
Enter security mode:

Firepower-chassis# scope security

**Step 2**
Delete the named key ring:

Firepower-chassis /security # delete keyring \textit{name}

**Step 3**
Commits the transaction:

Firepower-chassis /security # commit.buffer

**Example**

The following example deletes a key ring:

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

Deleting a Trusted Point

**Before you begin**

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

**Procedure**

**Step 1**
Enters security mode:

Firepower-chassis# scope security

**Step 2**
Delete the named trusted point:

Firepower-chassis /security # delete trustpoint \textit{name}

**Step 3**
Commits the transaction:
Example

The following example deletes a trusted point:

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

Disabling HTTPS

Procedure

1. Enter system mode:
   Firepower-chassis# scope system
2. Enter system services mode:
   Firepower-chassis /system # scope services
3. Disable the HTTPS service:
   Firepower-chassis /system/services # disable https
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
```

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

Step 1
Enter security mode:
Firepower-chassis# scope security

Step 2
Enter security LDAP mode:
Firepower-chassis /security # scope ldap

Step 3
Restrict database searches to records that contain the specified attribute:
Firepower-chassis /security/ldap # set attribute attribute

Step 4
Restrict database searches to records that contain the specified distinguished name:
Firepower-chassis /security/ldap # set basedn distinguished-name

Step 5
Restrict database searches to records that contain the specified filter:
Firepower-chassis /security/ldap # set filter filter

Step 6
Set the time interval the system should wait for a response from the LDAP server before noting the server as down:
Firepower-chassis /security/ldap # set timeout seconds

Step 7
Commit the transaction to the system configuration:
Firepower-chassis /security/ldap # commit-buffer

Example

The following example sets the LDAP attribute to CiscoAvPair, the base distinguished name to "DC=cisco-firepower-aaa3,DC=qalab,DC=com", the filter to sAMAccountName=$userid, and the timeout interval to 5 seconds, and commits the transaction:

Firepower-chassis# scope security
Firepower-chassis /security # scope ldap
Firepower-chassis /security/ldap # set attribute CiscoAvPair
Firepower-chassis /security/ldap* # set basedn "DC=cisco-firepower-aaa3,DC=qalab,DC=com"
Firepower-chassis /security/ldap* # set filter sAMAccountName=$userid
Firepower-chassis /security/ldap* # set timeout 5
Firepower-chassis /security/ldap # commit-buffer
Firepower-chassis /security/ldap #

---

**Note**

User login will fail if the userdn for an LDAP user exceeds 255 characters.

---

**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**

1. **Step 1**
   - Enter security mode:
     
     ```
     Firepower-chassis# scope security
     ```

2. **Step 2**
   - Enter security LDAP mode:
     
     ```
     Firepower-chassis /security # scope ldap
     ```

3. **Step 3**
   - Create an LDAP server instance and enter security LDAP server mode:
     
     ```
     Firepower-chassis /security/ldap # create server server-name
     ```
     - If SSL is enabled, the `server-name`, typically an IP address or FQDN, must exactly match a Common Name (CN) in the LDAP server's security certificate. Unless an IP address is specified, a DNS server must be configured.

4. **Step 4**
   - (Optional) Set an LDAP attribute that stores the values for the user roles and locales:
     
     ```
     Firepower-chassis /security/ldap/server # set attribute attr-name
     ```
     - 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 for LDAP providers.

5. **Step 5**
   - (Optional) Set 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:
     
     ```
     Firepower-chassis /security/ldap/server # set basedn basedn-name
     ```
Step 6  (Optional) Set the distinguished name (DN) for an LDAP database account that has read and search permissions for all objects under the base DN:

Firepower-chassis /security/ldap/server # set binddn binddn-name

The maximum supported string length is 255 ASCII characters.

Step 7  (Optional) Restrict the LDAP search to user names that match the defined filter.

Firepower-chassis /security/ldap/server # set filter filter-value

This value is required unless a default filter has been set for LDAP providers.

Step 8  Specify the password for the LDAP database account specified for Bind DN:

Firepower-chassis /security/ldap/server # set password

You can enter any standard ASCII characters except for space, § (section sign), ? (question mark), or = (equal sign).

To set the password, press Enter after typing the set password command and enter the key value at the prompt.

Step 9  (Optional) Specify the order in which the Firepower eXtensible Operating System uses this provider to authenticate users:

Firepower-chassis /security/ldap/server # set order order-num

Step 10  (Optional) Specify the port used to communicate with the LDAP server. The standard port number is 389.

Firepower-chassis /security/ldap/server # set port port-num

Step 11  Enable or disable the use of encryption when communicating with the LDAP server:

Firepower-chassis /security/ldap/server # set ssl {yes | no}

The options are as follows:

- yes — Encryption is required. If encryption cannot be negotiated, the connection fails.
- no — Encryption is disabled. Authentication information is sent as clear text.

LDAP uses STARTTLS. This allows encrypted communication using port 389.

Step 12  Specify the length of time in seconds the system should spend trying to contact the LDAP database before it times out:

Firepower-chassis /security/ldap/server # set timeout timeout-num

Enter an integer from 1 to 60 seconds, or enter 0 (zero) to use the global timeout value specified for LDAP providers. The default is 30 seconds.

Step 13  Specify the vendor that is providing the LDAP provider or server details:

Firepower-chassis /security/ldap/server # set vendor {ms-ad | openldap}
The options are as follows:

- **ms-ad**—LDAP provider is Microsoft Active Directory
- **openldap**—LDAP provider is not Microsoft Active Directory

**Step 14**
Commit the transaction to the system configuration:

```
Firepower-chassis/security/ldap/server# commit-buffer
```

**Example**
The following example creates an LDAP server instance named 10.193.169.246, configures the binddn, password, order, port, SSL settings, vendor attribute, and commits the transaction:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope ldap
Firepower-chassis /security/ldap* # create server 10.193.169.246
Firepower-chassis /security/ldap/server* # set binddn
"cn=Administrator,cn=Users,DC=cisco-firepower-aaa3,DC=qalab,DC=com"
Firepower-chassis /security/ldap/server* # set password
Enter the password:
Confirm the password:
Firepower-chassis /security/ldap/server* # set order 2
Firepower-chassis /security/ldap/server* # set port 389
Firepower-chassis /security/ldap/server* # set ssl yes
Firepower-chassis /security/ldap/server* # set timeout 30
Firepower-chassis /security/ldap/server* # set vendor ms-ad
Firepower-chassis /security/ldap/server* # commit-buffer
Firepower-chassis /security/ldap/server #
```

The following example creates an LDAP server instance named 12:31:71:1231:45b1:0011:011:900, configures the binddn, password, order, port, SSL settings, vendor attribute, and commits the transaction:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope ldap
Firepower-chassis /security/ldap/server* # set binddn
"cn=Administrator,cn=Users,DC=cisco-firepower-aaa3,DC=qalab,DC=com"
Firepower-chassis /security/ldap/server* # set password
Enter the password:
Confirm the password:
Firepower-chassis /security/ldap/server* # set order 1
Firepower-chassis /security/ldap/server* # set port 389
Firepower-chassis /security/ldap/server* # set ssl yes
Firepower-chassis /security/ldap/server* # set timeout 45
Firepower-chassis /security/ldap/server* # set vendor ms-ad
Firepower-chassis /security/ldap/server* # commit-buffer
Firepower-chassis /security/ldap/server #
```
Deleting an LDAP Provider

Procedure

Step 1 Enter security mode:
Firepower-chassis# scope security

Step 2 Enter security LDAP mode:
Firepower-chassis /security # scope ldap

Step 3 Delete the specified server:
Firepower-chassis /security/ldap # delete server serv-name

Step 4 Commit the transaction to the system configuration:
Firepower-chassis /security/ldap # commit-buffer

Example
The following example deletes the LDAP server called ldap1 and commits the transaction:

Firepower-chassis# scope security
Firepower-chassis /security # scope ldap
Firepower-chassis /security/ldap # delete server ldap1
Firepower-chassis /security/ldap* # commit-buffer
Firepower-chassis /security/ldap #

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.

Procedure

Step 1 Enter security mode:
Firepower-chassis# scope security

Step 2 Enter security RADIUS mode:
Firepower-chassis /security # scope radius

Step 3 (Optional) Specify the number of times to retry communicating with the RADIUS server before noting the server as down:
Firepower-chassis /security/radius # set retries retry-num

**Step 4**  
(Optional) Set the time interval the system should wait for a response from the RADIUS server before noting the server as down:

Firepower-chassis /security/radius # set timeout seconds

**Step 5**  
Commit the transaction to the system configuration:

Firepower-chassis /security/radius # commit-buffer

---

**Example**

The following example sets the RADIUS retries to 4, sets the timeout interval to 30 seconds, and commits the transaction:

```plaintext
Firepower-chassis# scope security  
Firepower-chassis /security # scope radius  
Firepower-chassis /security/radius # set retries 4
Firepower-chassis /security/radius* # set timeout 30  
Firepower-chassis /security/radius* # commit-buffer  
Firepower-chassis /security/radius #
```

**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**  
Enter security mode:

Firepower-chassis# scope security

**Step 2**  
Enter security RADIUS mode:

Firepower-chassis /security # scope radius

**Step 3**  
Create a RADIUS server instance and enter security RADIUS server mode:

Firepower-chassis /security/radius # create server server-name

**Step 4**  
(Optional) Specify the port used to communicate with the RADIUS server.

Firepower-chassis /security/radius/server # set authport authport-num

**Step 5**  
Set the RADIUS server key:

Firepower-chassis /security/radius/server # set key

To set the key value, press Enter after typing the set key command and enter the key value at the prompt.
Step 6  (Optional) Specify when in the order this server will be tried:
Firepower-chassis /security/radius/server # set order order-num

Step 7  (Optional) Set the number of times to retry communicating with the RADIUS server before noting the server as down:
Firepower-chassis /security/radius/server # set retries retry-num

Step 8  Specify the time interval that the system should wait for a response from the RADIUS server before noting the server as down:
Firepower-chassis /security/radius/server # set timeout seconds

Tip    It is recommended that you configure a higher Timeout value if you select two-factor authentication for RADIUS providers.

Step 9  Commit the transaction to the system configuration:
Firepower-chassis /security/radius/server # commit-buffer

Example
The following example creates a server instance named radiusserv7, sets the authentication port to 5858, sets the key to radiuskey321, sets the order to 2, sets the retries to 4, sets the timeout to 30, enables two-factor authentication, and commits the transaction:

Firepower-chassis# scope security
Firepower-chassis /security # scope radius
Firepower-chassis /security/radius # create server radiusserv7
Firepower-chassis /security/radius/server* # set authport 5858
Firepower-chassis /security/radius/server* # set key
Enter the key: radiuskey321
Confirm the key: radiuskey321
Firepower-chassis /security/radius/server* # set order 2
Firepower-chassis /security/radius/server* # set retries 4
Firepower-chassis /security/radius/server* # set timeout 30
Firepower-chassis /security/radius/server* # commit-buffer

Deleting a RADIUS Provider

Procedure

Step 1  Enter security mode:
Firepower-chassis# scope security

Step 2  Enter security RADIUS mode:
Firepower-chassis /security # scope RADIUS

Step 3  Delete the specified server:
Step 4
Commit the transaction to the system configuration:
Firepower-chassis /security/radius # commit-buffer

---

**Example**
The following example deletes the RADIUS server called radius1 and commits the transaction:

```plaintext
Firepower-chassis# scope security
Firepower-chassis /security # scope radius
Firepower-chassis /security/radius # delete server radius1
Firepower-chassis /security/radius* # commit-buffer
Firepower-chassis /security/radius #
```

---

**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**
Enter security mode:
Firepower-chassis# scope security

**Step 2**
Enter security TACACS+ mode:
Firepower-chassis /security # scope tacacs

**Step 3**
(Optional) Set the time interval the system should wait for a response from the TACACS+ server before noting the server as down:
Firepower-chassis /security/tacacs # set timeout seconds

**Step 4**
Commit the transaction to the system configuration:
Firepower-chassis /security/tacacs # commit-buffer

---

**Example**
The following example sets the TACACS+ timeout interval to 45 seconds and commits the transaction:

```plaintext
Firepower-chassis# scope security
Firepower-chassis /security # scope tacacs
Firepower-chassis /security/tacacs # set timeout 45
```
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** Enter security mode:
Firepower-chassis# scope security

**Step 2** Enter security TACACS+ mode:
Firepower-chassis /security # scope tacacs

**Step 3** Create a TACACS+ server instance and enter security TACACS+ server mode:
Firepower-chassis /security/tacacs # create server server-name

**Step 4** Specify the TACACS+ server key:
Firepower-chassis /security/tacacs/server # set key
To set the key value, press Enter after typing the set key command and enter the key value at the prompt.

**Step 5** (Optional) Specify when in the order this server will be tried:
Firepower-chassis /security/tacacs/server # set order order-num

**Step 6** Specify the time interval that the system should wait for a response from the TACACS+ server before noting the server as down:
Firepower-chassis /security/tacacs/server # set timeout seconds

**Tip** It is recommended that you configure a higher timeout value if you select two-factor authentication for TACACS+ providers.

**Step 7** (Optional) Specify the port used to communicate with the TACACS+ server:
Firepower-chassis /security/tacacs/server # set port port-num

**Step 8** Commit the transaction to the system configuration:
Firepower-chassis /security/tacacs/server # commit-buffer
Example

The following example creates a server instance named tacacsserv680, sets the key to tacacskey321, sets the order to 4, sets the authentication port to 5859, and commits the transaction:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope tacacs
Firepower-chassis /security/tacacs # create server tacacsserv680
Firepower-chassis /security/tacacs/server* # set key
Enter the key: tacacskey321
Firepower-chassis /security/tacacs/server* # set order 4
Firepower-chassis /security/tacacs/server* # set port 5859
Firepower-chassis /security/tacacs/server* # commit-buffer
```

Deleting a TACACS+ Provider

Procedure

Step 1 Enter security mode:

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

Step 2 Enter security TACACS+ mode:

```
Firepower-chassis /security # scope tacacs
```

Step 3 Delete the specified server:

```
Firepower-chassis /security/tacacs # delete server serv-name
```

Step 4 Commit the transaction to the system configuration:

```
Firepower-chassis /security/tacacs # commit-buffer
```

Example

The following example deletes the TACACS+ server called tacacs1 and commits the transaction:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope tacacs
Firepower-chassis /security/tacacs # delete server tacacs1
Firepower-chassis /security/tacacs # commit-buffer
```

Configuring Syslog

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

**Procedure**

**Step 1**
Enter monitoring mode:
Firepower-chassis# **scope monitoring**

**Step 2**
Enable or disable the sending of syslogs to the console:
Firepower-chassis /monitoring # {**enable** | **disable**} **syslog console**

**Step 3**
(Optional) Select the lowest message level that you want displayed. If syslogs are enabled, the system displays that level and above on the console. The level options are listed in order of decreasing urgency. The default level is Critical.
Firepower-chassis /monitoring # **set syslog console level** {emergencies | alerts | critical}

**Step 4**
Enable or disable the monitoring of syslog information by the operating system:
Firepower-chassis /monitoring # {**enable** | **disable**} **syslog monitor**

**Step 5**
(Optional) Select the lowest message level that you want displayed. If the monitor state is enabled, the system displays that level and above. The level options are listed in order of decreasing urgency. The default level is Critical.
Firepower-chassis /monitoring # **set syslog monitor level** {emergencies | alerts | critical | errors | warnings | notifications | information | debugging}

**Note**
Messages at levels below Critical are displayed on the terminal monitor only if you have entered the **terminal monitor** command.

**Step 6**
Enable or disable the writing of syslog information to a syslog file:
Firepower-chassis /monitoring # {**enable** | **disable**} **syslog file**

**Step 7**
Specify the name of the file in which the messages are logged. Up to 16 characters are allowed in the file name.
Firepower-chassis /monitoring # **set syslog file name** filename

**Step 8**
(Optional) Select the lowest message level that you want stored to a file. If the file state is enabled, the system stores that level and above in the syslog file. The level options are listed in order of decreasing urgency. The default level is Critical.
Firepower-chassis /monitoring # **set syslog file level** {emergencies | alerts | critical | errors | warnings | notifications | information | debugging}

**Step 9**
(Optional) Specify the maximum file size, in bytes, before the system begins to write over the oldest messages with the newest ones. The range is 4096 to 4194304 bytes.
Firepower-chassis /monitoring # **set syslog file size** filesize

**Step 10**
Configure sending of syslog messages to up to three external syslog servers:
a) Enable or disable the sending of syslog messages to up to three external syslog servers:
Firepower-chassis/monitoring # {enable | disable} syslog remote-destination {server-1 | server-2 | server-3}

b) (Optional) Select the lowest message level that you want stored to the external log. If the remote-destination is enabled, the system sends that level and above to the external server. The level options are listed in order of decreasing urgency. The default level is Critical.

Firepower-chassis/monitoring # set syslog remote-destination {server-1 | server-2 | server-3} level {emergencies | alerts | critical | errors | warnings | notifications | information | debugging}

c) Specify the hostname or IP address of the specified remote syslog server. Up to 256 characters are allowed in the hostname.

Firepower-chassis/monitoring # set syslog remote-destination {server-1 | server-2 | server-3} hostname hostname

d) (Optional) Specify the facility level contained in the syslog messages sent to the specified remote syslog server.

Firepower-chassis/monitoring # set syslog remote-destination {server-1 | server-2 | server-3} facility {local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7}

Step 11
Configure the local sources. Enter the following command for each of the local sources you want to enable or disable:

Firepower-chassis /monitoring # {enable | disable} syslog source {audits | events | faults}

This can be one of the following:
• audits—Enables or disables the logging of all audit log events.
• events—Enables or disables the logging of all system events.
• faults—Enables or disables the logging of all system faults.

Step 12
Commit the transaction:

Firepower-chassis /monitoring # commit-buffer

Example
This example shows how to enable the storage of syslog messages in a local file and commits the transaction:

Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # disable syslog console
Firepower-chassis /monitoring* # disable syslog monitor
Firepower-chassis /monitoring* # enable syslog file
Firepower-chassis /monitoring* # set syslog file name SysMsgsFirepower
Firepower-chassis /monitoring* # set syslog file level notifications
Firepower-chassis /monitoring* # set syslog file size 4194304
Firepower-chassis /monitoring* # disable syslog remote-destination server-1
Firepower-chassis /monitoring* # disable syslog remote-destination server-2
Firepower-chassis /monitoring* # disable syslog remote-destination server-3
Firepower-chassis /monitoring* # commit-buffer
Firepower-chassis /monitoring #
# 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**

Enter system mode:

```
Firepower-chassis# scope system
```

**Step 2**

Enter system services mode:

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

**Step 3**

To create or delete a DNS server, enter the appropriate command as follows:

- To configure the system to use a DNS server with the specified IPv4 or IPv6 address:

  ```
  Firepower-chassis /system/services# create dns {ip-addr | ip6-addr}
  ```

- To delete a DNS server with the specified IPv4 or IPv6 address:

  ```
  Firepower-chassis /system/services# delete dns {ip-addr | ip6-addr}
  ```

**Step 4**

Commit the transaction to the system configuration:

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

## Example

The following example configures a DNS server with the IPv4 address 192.168.200.105 and commits the transaction:

```
Firepower-chassis# scope system
Firepower-chassis /system# scope services
Firepower-chassis /system/services# create dns 192.168.200.105
Firepower-chassis /system/services*# commit-buffer
Firepower-chassis /system/services#
```

The following example configures a DNS server with the IPv6 address 2001:db8::22:F376:FF3B:AB3F and commits the transaction:

```
Firepower-chassis# scope system
Firepower-chassis /system# scope services
Firepower-chassis /system/services# create dns 2001:db8::22:F376:FF3B:AB3F
Firepower-chassis /system/services*# commit-buffer
Firepower-chassis /system/services#
```
Configuring DNS Servers

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # create dns 2001:db8::22:F376:FF3B:AB3F
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

The following example deletes the DNS server with the IP address 192.168.200.105 and commits the transaction:

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # delete dns 192.168.200.105
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```
Chapter 8

Interface Management

- About Firepower Interfaces, on page 99
- Guidelines and Limitations for Firepower Interfaces, on page 100
- Configure Interfaces, on page 100
- Monitoring Interfaces, on page 107

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 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 55. 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 99.

- 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.

**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

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
</table>
| 1     | Enter interface mode.  
scope eth-uplink  
scope fabric a |
| 2     | Enable the interface.  
enter interface interface_id  
enable |
| 3     | (Optional) Set the interface type.  
set port-type {data | mgmt | cluster} |
| 4     | Enable or disable autonegotiation, if supported for your interface.  
set auto-negotiation {on | off} |
| 5     | Set the interface speed.  
set admin-speed {10mbps | 100mbps | 1gbps | 10gbps | 40gbps | 100gbps} |

Example:

```
Firepower /eth-uplink/fabric # enter interface Ethernet1/8
Firepower /eth-uplink/fabric/interface # enable
```

Note: Interfaces that are already a member of a port-channel cannot be modified individually. If you use the `enter interface` or `scope interface` command on an interface that is a member of a port channel, you will receive an error stating that the object does not exist. You should edit interfaces using the `enter interface` command before you add them to a port-channel.

Step 3 (Optional) Set the interface type.

```
Firepower /eth-uplink/fabric/interface # set port-type mgmt
```

The `data` keyword is the default type. Do not choose the `cluster` keyword; by default, the cluster control link is automatically created on Port-channel 48.

Step 4 Enable or disable autonegotiation, if supported for your interface.

```
Firepower /eth-uplink/fabric/interface* # set auto-negotiation off
```

Step 5 Set the interface speed.

```
Firepower /eth-uplink/fabric/interface# set admin-speed 1gbps
```

Example:
**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.

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

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

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

Procedure

**Step 1** Enter interface mode:
```
scope eth-uplink
scope fabric a
```

**Step 2** Create the port-channel:
```
create port-channel id
enable
```

**Step 3** Assign member interfaces:
```
create member-port interface_id
```
**Example:**
```
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
```

**Step 4** (Optional) Set the interface type.
```
set port-type {data | mgmt | cluster}
```
**Example:**
```
Firepower /eth-uplink/fabric/port-channel* # set port-type data
```

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

**Step 5** (Optional) Set the interface speed for all members of the port-channel.
```
set speed {10mbps | 100mbps | 1gbps | 10gbps | 40gbps | 100gbps}
```
**Example:**
```
Firepower /eth-uplink/fabric/port-channel* # set speed 1gbps
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 To create a new breakout, use the following commands:
   a) Enter cabling mode:
      scope cabling
      scope fabric a
   b) Create the breakout:
      create breakout network_module_slot port
      Example:
      Firepower /cabling/fabric/ # create breakout 2 1
   c) Commit the configuration:
commit-buffer

This will cause an automatic reboot. If you are configuring more than one breakout, you should create all of them before you issue the commit-buffer command.

Step 2

To enable/configure the breakout ports, use the following commands:

a) Enter interface mode:
   - scope eth-uplink
   - scope fabric a
   - scope aggr-interface network_module_slot port

   **Note** Interfaces that are already a member of a port-channel cannot be modified individually. If you use the `enter interface` or `scope interface` command on an interface that is a member of a port channel, you will receive an error stating that the object does not exist. You should edit interfaces using the `enter interface` command before you add them to a port-channel.

b) Use the `set` command to configure the interface speed and port type.
   Use the `enable` or `disable` command to set the administrative state of the interface.

c) Commit the configuration:
   - commit-buffer

---

**Configure a Flow Control Policy**

Flow control policies determine whether the Ethernet ports send and receive IEEE 802.3x pause frames when the receive buffer for a port fills. These pause frames request that the transmitting port stop sending data for a few milliseconds until the buffer clears. For flow control to work between devices, you must enable the corresponding receive and send flow control parameters for both devices.

The default policy disables send and receive control, and sets the priority to autonegotiate.

**Procedure**

**Step 1**

Enter eth-uplink and then flow-control mode.

- scope eth-uplink
- scope flow-control

**Example:**

```plaintext
firepower-4110# scope eth-uplink
firepower-4110 /eth-uplink # scope flow-control
firepower-4110 /eth-uplink/flow-control #
```

**Step 2**

Edit or create a flow control policy.

- enter policy name
If you want to edit the default policy, enter `default` for the name.

**Example:**

```bash
firmware-4110 /eth-uplink/flow-control # enter policy default
firmware-410 /eth-uplink/flow-control/policy* #
```

**Step 3**

Set the priority.

```bash
set prio {auto | on}
```

The priority sets whether to negotiate or enable PPP for this link.

**Example:**

```bash
firmware-4110 /eth-uplink/flow-control/policy* # set prio on
```

**Step 4**

Enable or disable flow control receive pauses.

```bash
set receive {on | off}
```

- **on**—Pause requests are honored and all traffic is halted on that uplink port until the network cancels the pause request.
- **off**—Pause requests from the network are ignored and traffic flow continues as normal.

**Example:**

```bash
firmware-4110 /eth-uplink/flow-control/policy* # set receive on
```

**Step 5**

Enable or disable flow control send pauses.

```bash
set send {on | off}
```

- **on**—The Firepower 9300 sends a pause request to the network if the incoming packet rate becomes too high. The pause remains in effect for a few milliseconds before traffic is reset to normal levels.
- **off**—Traffic on the port flows normally regardless of the packet load.

**Example:**

```bash
firmware-4110 /eth-uplink/flow-control/policy* # set send on
```

**Step 6**

Save the configuration.

```bash
commit-buffer
```

**Example:**

```bash
firmware-4110 /eth-uplink/flow-control/policy* # commit-buffer
firmware-4110 /eth-uplink/flow-control/policy#
```
Example

The following example configures a flow control policy.

```
firepower-4110# scope eth-uplink
firepower-4110 /eth-uplink # scope flow-control
firepower-4110 /eth-uplink/flow-control # enter policy FlowControlPolicy23
firepower-4110 /eth-uplink/flow-control/policy* # set prio auto
firepower-4110 /eth-uplink/flow-control/policy* # set receive on
firepower-4110 /eth-uplink/flow-control/policy* # set send on
firepower-4110 /eth-uplink/flow-control/policy* # commit-buffer
firepower-4110 /eth-uplink/flow-control/policy#
```

Monitoring Interfaces

- show interface

  Shows interface status.

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

```
Firepower# scope eth-uplink
Firepower /eth-uplink # scope fabric a
Firepower /eth-uplink/fabric # show interface

Interface:
Port Name Port Type Admin State Oper State State Reason
----------------- ------------------ ----------- ---------------- -------------
Ethernet1/1 Mgmt Enabled Up
Ethernet1/2 Data Enabled Link Down Link failure or not-connected
Ethernet1/3 Data Enabled Up
Ethernet1/4 Data Enabled Sfp Not Present Unknown
Ethernet1/6 Data Enabled Sfp Not Present Unknown
Ethernet1/7 Data Enabled Sfp Not Present Unknown
Ethernet1/8 Data Disabled Sfp Not Present Unknown
Ethernet2/1 Data Enabled Up
Ethernet2/2 Data Enabled Up
Ethernet2/4 Data Enabled Up
Ethernet2/5 Data Enabled Up
Ethernet2/6 Data Enabled Up
Ethernet3/2 Data Enabled Up
Ethernet3/4 Data Enabled Up
```
Logical Devices

• About Logical Devices, on page 109
• Requirements and Prerequisites for Logical Devices, on page 110
• Guidelines and Limitations for Logical Devices, on page 111
• Add a Standalone Logical Device, on page 115
• Add a High Availability Pair, on page 120
• Add a Cluster, on page 121
• Manage Logical Devices, on page 132
• Monitoring Logical Devices, on page 138
• Examples for Inter-Site Clustering, on page 139
• History for Logical Devices, on page 141

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.

Note For the Firepower 9300, all modules must belong to the cluster. You cannot create a standalone logical device on one security module and then create a cluster using the remaining 2 security modules.

Requirements and Prerequisites for Logical Devices

See the following sections for requirements and prerequisites.

Requirements and Prerequisites for Clustering

Inter-Chassis Clustering Hardware and Software Requirements

All chassis in a cluster:

• All security modules must be the same type. You can have different quantities of installed security modules in each chassis, although all modules present in the chassis must belong to the cluster including any empty slots.

• Must run the identical FXOS software except at the time of an image upgrade.

• Must include the same interface configuration for interfaces you assign to the cluster, such as the same Management interface, EtherChannels, active interfaces, speed and duplex, and so on. You can use different network module types on the chassis as long as the capacity matches for the same interface IDs and interfaces can successfully bundle in the same spanned EtherChannel. Note that all data interfaces must be EtherChannels in inter-chassis clustering. If you change the interfaces in FXOS after you enable clustering (by adding or removing interface modules, or configuring EtherChannels, for example), then perform the same changes on each chassis, starting with the slave units, and ending with the master.

• Must use the same NTP server. Do not set the time manually.

• ASA: Each FXOS chassis must be registered with the License Authority or satellite server. There is no extra cost for slave units. For Firepower Threat Defense, all licensing is handled by the Firepower Management Center.

Switch Requirements for Inter-Chassis Clustering

• Be sure to complete the switch configuration and successfully connect all the EtherChannels from the chassis to the switch(es) before you configure clustering on the Firepower 9300 chassis.

• For a list of supported switches, see Cisco FXOS Compatibility.

Sizing the Data Center Interconnect for Inter-Site Clustering

You should reserve bandwidth on the data center interconnect (DCI) for cluster control link traffic equivalent to the following calculation:
If the number of members differs at each site, use the larger number for your calculation. The minimum bandwidth for the DCI should not be less than the size of the cluster control link for one member.

For example:

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

  Reserved DCI bandwidth = 5 Gbps \((2/2 \times 5 \text{ Gbps})\).

- For 6 members at 3 sites, the size increases:
  - 6 cluster members total
  - 3 members at site 1, 2 members at site 2, and 1 member at site 3
  - 10 Gbps cluster control link per member

  Reserved DCI bandwidth = 15 Gbps \((3/2 \times 10 \text{ Gbps})\).

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

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

---

**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 135.

**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

Switches for Inter-Chassis Clustering
• For the ASR 9006, if you want to set a non-default MTU, set the ASR interface MTU to be 14 bytes higher than the cluster device MTU. Otherwise, OSPF adjacency peering attempts may fail unless the mtu-ignore option is used. Note that the cluster device MTU should match the ASR IPv4 MTU.
• On the switch(es) for the cluster control link interfaces, you can optionally enable Spanning Tree PortFast on the switch ports connected to the cluster unit to speed up the join process for new units.
• When you see slow bundling of a Spanned EtherChannel on the switch, you can enable LACP rate fast for an individual interface on the switch. Note that some switches, such as the Nexus series, do not support LACP rate fast when performing in-service software upgrades (ISSUs), so we do not recommend using ISSUs with clustering.
• On the switch, we recommend that you use one of the following EtherChannel load-balancing algorithms: source-dest-ip or source-dest-ip-port (see the Cisco Nexus OS and Cisco IOS port-channel load-balance command). Do not use a vlan keyword in the load-balance algorithm because it can cause unevenly distributed traffic to the devices in a cluster.
• If you change the load-balancing algorithm of the EtherChannel on the switch, the EtherChannel interface on the switch temporarily stops forwarding traffic, and the Spanning Tree Protocol restarts. There will be a delay before traffic starts flowing again.
• Switches on the cluster control link path should not verify the L4 checksum. Redirected traffic over the cluster control link does not have a correct L4 checksum. Switches that verify the L4 checksum could cause traffic to be dropped.
• Port-channel bundling downtime should not exceed the configured keepalive interval.
• On Supervisor 2T EtherChannels, the default hash distribution algorithm is adaptive. To avoid asymmetric traffic in a VSS design, change the hash algorithm on the port-channel connected to the cluster device to fixed:
  router(config)# port-channel id hash-distribution fixed
Do not change the algorithm globally; you may want to take advantage of the adaptive algorithm for the VSS peer link.

EtherChannels for Inter-Chassis Clustering
• For connecting switches, set the EtherChannel mode to Active; On mode is not supported on the Firepower 9300 chassis, even for the cluster control link.
• FXOS EtherChannels have the LACP rate set to fast by default. Some switches, such as the Nexus series, do not support LACP rate fast when performing in-service software upgrades (ISSUs), so we do not recommend using ISSUs with clustering.

• In Catalyst 3750-X Cisco IOS software versions earlier than 15.1(1)S2, the cluster unit did not support connecting an EtherChannel to a switch stack. With default switch settings, if the cluster unit EtherChannel is connected cross stack, and if the master switch is powered down, then the EtherChannel connected to the remaining switch will not come up. To improve compatibility, set the stack-mac persistent timer command to a large enough value to account for reload time; for example, 8 minutes or 0 for indefinite. Or, you can upgrade to more a more stable switch software version, such as 15.1(1)S2.

• Spanned vs. Device-Local EtherChannel Configuration—Be sure to configure the switch appropriately for Spanned EtherChannels vs. Device-local EtherChannels.
  
  • Spanned EtherChannels—For cluster unit Spanned EtherChannels, which span across all members of the cluster, the interfaces are combined into a single EtherChannel on the switch. Make sure each interface is in the same channel group on the switch.

  ![Diagram](image)

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

See the following guidelines for inter-site clustering:

- The cluster control link latency must be less than 20 ms round-trip time (RTT).
- The cluster control link must be reliable, with no out-of-order or dropped packets; for example, you should use a dedicated link.
- Do not configure connection rebalancing; you do not want connections rebalanced to cluster members at a different site.
- The cluster implementation does not differentiate between members at multiple sites for incoming connections; therefore, connection roles for a given connection may span across sites. This is expected behavior.
- For transparent mode, if the cluster is placed between a pair of inside and outside routers (AKA North-South insertion), you must ensure that both inside routers share a MAC address, and also that both outside routers share a MAC address. When a cluster member at site 1 forwards a connection to a member at site 2, the destination MAC address is preserved. The packet will only reach the router at site 2 if the MAC address is the same as the router at site 1.
• For transparent mode, if the cluster is placed between data networks and the gateway router at each site for firewallsing between internal networks (AKA East-West insertion), then each gateway router should use a First Hop Redundancy Protocol (FHRP) such as HSRP to provide identical virtual IP and MAC address destinations at each site. The data VLANs are extended across the sites using Overlay Transport Virtualization (OTV), or something similar. You need to create filters to prevent traffic that is destined to the local gateway router from being sent over the DCI to the other site. If the gateway router becomes unreachable at one site, you need to remove any filters so traffic can successfully reach the other site’s gateway.

• For routed mode using Spanned EtherChannel, configure site-specific MAC addresses. Extend the data VLANs across the sites using OTV, or something similar. You need to create filters to prevent traffic that is destined to the global MAC address from being sent over the DCI to the other site. If the cluster becomes unreachable at one site, you need to remove any filters so traffic can successfully reach the other site’s cluster units. Dynamic routing is not supported when an inter-site cluster acts as the first hop router for an extended segment.

Additional Guidelines

• 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 120.

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 135.

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 44), and then download that image to the Firepower 9300 chassis (see Downloading a Logical Device Software Image to the Firepower 9300 chassis, on page 47).
- 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 (in FXOS, you might see it displayed as MGMT, management0, or other similar names).

**Procedure**

**Step 1**

Enter security services mode.

```
scope ssa
```

**Example:**

```
Firepower# scope ssa
Firepower /ssa #
```

**Step 2**

Set the application instance image version.

a) View available images. Note the Version number that you want to use.

```
show app
```

**Example:**

```
Firepower /ssa # show app

<table>
<thead>
<tr>
<th>Name</th>
<th>Version</th>
<th>Author</th>
<th>Supported Deploy Types</th>
<th>CSP Type</th>
<th>Is Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>asa</td>
<td>9.9.1</td>
<td>cisco</td>
<td>Native</td>
<td>Application No</td>
<td></td>
</tr>
<tr>
<td>asa</td>
<td>9.10.1</td>
<td>cisco</td>
<td>Native</td>
<td>Application Yes</td>
<td></td>
</tr>
<tr>
<td>ftd</td>
<td>6.2.3</td>
<td>cisco</td>
<td>Native</td>
<td>Application Yes</td>
<td></td>
</tr>
</tbody>
</table>
```

b) Set the scope to the security module/engine slot.

```
scope slot slot_id
```

The `slot_id` is 1, 2, or 3 for the Firepower 9300.

**Example:**

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot #
```

c) Create the application instance.

```
enter app-instance asa
```

**Example:**

```
Firepower /ssa/slot # enter app-instance asa
Firepower /ssa/slot/app-instance* #
```

d) Set the ASA image version.

```
set startup-version version
```
Logical Devices

Add a Standalone ASA

**Example:**

Firepower /ssa/slot/app-instance* # set startup-version 9.10.1

e) Exit to slot mode.
   
   exit
   
   **Example:**
   
   Firepower /ssa/slot/app-instance* # exit
   Firepower /ssa/slot* #

f) Exit to ssa mode.
   
   exit
   
   **Example:**
   
   Firepower /ssa/slot* # exit
   Firepower /ssa* #

Step 3  
Create the logical device.

```markdown
enter logical-device device_name asa slot_id standalone
```

**Example:**

Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance asa ASA1
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* #

Step 4  
Assign the management and data interfaces to the logical device. Repeat for each interface.

```markdown
create external-port-link name interface_id asa
set description description
exit
```

- **name**—The name is used by the Firepower 9300 chassis supervisor; it is not the interface name used in the ASA configuration.
- **description**—Use quotes (") around phrases with spaces.

**Example:**
Step 5  Configure the management bootstrap information:

a)  Create the bootstrap object.

   create mgmt-bootstrap asa

   Example:

   Firepower /ssa/logical-device* # create mgmt-bootstrap asa
   Firepower /ssa/logical-device/mgmt-bootstrap* #

b)  Specify the admin password.

   create bootstrap-key-secret PASSWORD

   set value

   Enter a value: password

   Confirm the value: password

   exit

   Example:

   Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
   Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
   Enter a value: floppylampshade
   Confirm the value: floppylampshade
   Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
   Firepower /ssa/logical-device/mgmt-bootstrap* #

   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.

   Example:

   Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
   Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
   Enter a value: floppylampshade
   Confirm the value: floppylampshade
   Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
   Firepower /ssa/logical-device/mgmt-bootstrap* #

   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.

   Example:

   Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
   Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
   Enter a value: floppylampshade
   Confirm the value: floppylampshade
   Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
   Firepower /ssa/logical-device/mgmt-bootstrap* #

   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.

   Example:

   Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
   Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
   Enter a value: floppylampshade
   Confirm the value: floppylampshade
   Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
   Firepower /ssa/logical-device/mgmt-bootstrap* #

   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.

   Example:

   Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
   Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
   Enter a value: floppylampshade
   Confirm the value: floppylampshade
   Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
   Firepower /ssa/logical-device/mgmt-bootstrap* #

   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.

   Example:
d) Configure the IPv6 management interface settings.

```
create ipv6 slot_id default
set ip ip_address prefix-length prefix
set gateway gateway_address
```

**Example:**
```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
```

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
```

e) Exit the management bootstrap mode.

```
exit
```

**Example:**
```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
```

**Step 6**

Save the configuration.

```
commit-buffer
```

**Example:**
```
Firepower /ssa/logical-device* # commit-buffer
```

```
Firepower /ssa/logical-device #
```

**Example**
```
Firepower# scope ssa
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance asa MyDevice1
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* # create logical-device MyDevice1 asa 1 standalone
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 asa
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 asa
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
```
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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>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.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Allocate the same interfaces to each logical device.</td>
</tr>
<tr>
<td>Step 3</td>
<td>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.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enable High Availability on the logical devices.</td>
</tr>
<tr>
<td>Step 5</td>
<td>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.</td>
</tr>
</tbody>
</table>

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. You can also use inter-chassis clustering, where multiple chassis are grouped together.

Note

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

About Clustering on the Firepower 9300 Chassis

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

• Creates a cluster-control link (by default, port-channel 48) for unit-to-unit communication. For intra-chassis clustering, this link utilizes the Firepower 9300 backplane for cluster communications. For inter-chassis clustering, you need to manually assign physical interface(s) to this EtherChannel for communications between chassis.

• Creates the cluster bootstrap configuration within the application.

When you deploy the cluster, the 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. Some parts of the bootstrap configuration may be user-configurable within the application if you want to customize your clustering environment.

• Assigns data interfaces to the cluster as Spanned interfaces.

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

Note

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

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

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

Primary and Secondary Unit Roles

One member of the cluster is the primary unit. The primary unit is determined automatically. All other members are secondary units.
You must perform all configuration on the primary unit only; the configuration is then replicated to the secondary units.

**Cluster Control Link**

The cluster control link is automatically created using the Port-channel 48 interface. For intra-chassis clustering, this interface has no member interfaces. For inter-chassis clustering, you must add one or more interfaces to the EtherChannel. This Cluster type EtherChannel utilizes the Firepower 9300 backplane for cluster communications for intra-chassis clustering.

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

Cluster control link traffic includes both control and data traffic.

**Size the Cluster Control Link for Inter-Chassis Clustering**

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

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

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

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

---

**Note**

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

**Cluster Control Link Redundancy for Inter-Chassis Clustering**

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

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

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

Cluster Control Link Network

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

Management Network

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

Management Interface

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

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

**Spanned EtherChannels**

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

**Inter-Site Clustering**

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

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

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

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

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

- Sizing the Data Center Interconnect—Requirements and Prerequisites for Clustering, on page 110
- Inter-Site Guidelines—Clustering Guidelines and Limitations, on page 112
- Inter-Site Examples—Examples for Inter-Site Clustering, on page 139

Add an ASA Cluster

You can add a single Firepower 9300 chassis as an intra-chassis cluster, or add multiple chassis for inter-chassis clustering. For inter-chassis clustering, you must configure each chassis separately. Add the cluster on one chassis; you can then enter most of the same settings on the next chassis.

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**

Configure 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 102 or Configure a Physical Interface, on page 100.

All interfaces are assigned to the cluster by default. You can also add data interfaces to the cluster after you deploy.

For inter-chassis clustering, all data interfaces must be EtherChannels with at least one member interface. Add the EtherChannels on each chassis.

**Step 2**

Add a Management type interface or EtherChannel. See Add an EtherChannel (Port Channel), on page 102 or Configure a Physical Interface, on page 100.
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 (in FXOS, you might see the chassis management interface displayed as MGMT, management0, or other similar names).

**Step 3**  
Port-channel 48 is reserved as the cluster control link. For inter-chassis clustering, add at least one member interface to port-channel 48.

**Step 4**  
Enter security services mode:

```
scope ssa
```

Example:

```
Firepower # scope ssa
Firepower /ssa #
```

**Step 5**  
Create the cluster:

```
enter logical-device device_name asa slots clustered
```

- **device_name**—Used by the Firepower 9300 chassis supervisor to configure clustering settings and assign interfaces; it is not the cluster name used in the security module configuration. You must specify all three security modules, even if you have not yet installed the hardware.

- **slots**—Assigns the chassis modules to the cluster. For the Firepower 4100, specify 1. For the Firepower 9300, specify 1,2,3. 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.

Example:

```
Firepower /ssa # enter logical-device ASA1 asa 1,2,3 clustered
Firepower /ssa/logical-device* #
```

**Step 6**  
Create the management bootstrap object.

```
enter mgmt-bootstrap asa
```

Example:

```
Firepower /ssa/logical-device* # enter mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

**Step 7**  
Specify the admin user password.

```
enter bootstrap-key-secret PASSWORD
set value
exit
```

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

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.

Example:
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: happytuesday
Confirm the value: happytuesday
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #

**Step 8** Configure the cluster parameters:

**enter cluster-bootstrap**

**Example:**

Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* #

**Step 9** Set the cluster group name in the security module configuration.

**set service-type cluster_name**

**Example:**

Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* #

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

**Step 10** Set the cluster interface mode:

**set mode spanned-etherchannel**

**Example:**

Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* #

Spanned EtherChannel mode is the only supported mode.

**Step 11** Configure the management IP address information.

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

a) Configure a pool of Local IP addresses, one of which will be assigned to each cluster unit for the interface:

**set ipv4 pool start_ip end_ip**

**set ipv6 pool start_ip end_ip**

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) Configure the Main cluster IP address for the management interface:

**set virtual ipv4 ip_address mask mask**
set virtual ipv6 ip_address prefix-length prefix

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

c) Enter the network gateway address:

set ipv4 gateway ip_address
set ipv6 gateway ip_address

Example:

Firepower /ssa/logical-device/cluster-bootstrap* # set ipv4 gateway 10.1.1.254
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv4 pool 10.1.1.11 10.1.1.27
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv6 gateway 2001:DB8::AA
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv6 pool 2001:DB8::11 2001:DB8::27
Firepower /ssa/logical-device/cluster-bootstrap* # set virtual ipv4 10.1.1.1 mask 255.255.255.0
Firepower /ssa/logical-device/cluster-bootstrap* # set virtual ipv6 2001:DB8::1 prefix-length 64

Step 12  Set the chassis ID:

set chassis-id id

Each chassis in the cluster needs a unique ID.

Example:

Firepower /ssa/logical-device/cluster-bootstrap* # set chassis-id 1
Firepower /ssa/logical-device/cluster-bootstrap* #

Step 13  Configure an authentication key for control traffic on the cluster control link:

set key

Example:

Firepower /ssa/logical-device/cluster-bootstrap* # set key
Key: diamonddogs

You are prompted to enter the shared secret.

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 14  Exit the cluster bootstrap mode and logical device mode:

exit
exit

Step 15  View the available software versions and then set the version you want to use:

a) Show the available versions:

show app

Example:
/ssa # show app

Application:
Name  Version  Description  Author  Deploy Type  CSP Type  Is Default App
---------- ---------- ----------- ---------- ----------- ----------- --------------
asa  9.1.4.152  N/A  cisco  Native Application Yes
asa  9.4.2  N/A  cisco  Native Application No
asa  9.5.2.1  N/A  cisco  Native Application No

b) Enter app mode for the version you want to use:

    scope app asa version_number

c) Set this version as the default:

    set-default

d) Exit app mode:

    exit

Example:

/ssa* # scope app asa 9.5.2.1
/ssa/app* # set-default
/ssa/app* # exit
/ssa* #

Step 16 Commit the configuration:

commit-buffer

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

Step 17 To add another chassis to the cluster, repeat this procedure except you must configure a unique chassis-id; otherwise, use the same configuration for both chassis.

Step 18 Connect to the master unit ASA to customize your clustering configuration.

Example

For chassis 1:

    scope eth-uplink
    scope fabric a
    enter port-channel 1
    set port-type data
    enable
    enter member-port Ethernet1/1
    exit
    enter member-port Ethernet1/2
    exit
exit
enter port-channel 2
set port-type data
enable
enter member-port Ethernet1/3
exit
enter member-port Ethernet1/4
exit
exit
enter port-channel 3
set port-type data
enable
enter member-port Ethernet1/5
exit
enter member-port Ethernet1/6
exit
exit
enter port-channel 4
set port-type mgmt
enable
enter member-port Ethernet2/1
exit
enter member-port Ethernet2/2
exit
exit
enter port-channel 48
set port-type cluster
enable
enter member-port Ethernet2/3
exit
exit
exit
exit
commit-buffer

scope ssa
  enter logical-device ASA1 asa "1,2,3" clustered
  enter cluster-bootstrap
    set chassis-id 1
    set ipv4 gateway 10.1.1.254
    set ipv4 pool 10.1.1.11 10.1.1.27
    set ipv6 gateway 2001:DB8::AA
    set ipv6 pool 2001:DB8::11 2001:DB8::27
    set key
      Key: f8arscape
    set mode spanned-etherchannel
    set service-type cluster1
    set virtual ipv4 10.1.1.1 mask 255.255.255.0
    set virtual ipv6 2001:DB8::1 prefix-length 64
  exit
  scope app asa 9.5.2.1
  set-default
  exit
  commit-buffer

For chassis 2:

scope eth-uplink
scope fabric a
create port-channel 1
set port-type data
enable
create member-port Ethernet1/1
  exit
create member-port Ethernet1/2
  exit
exit
create port-channel 2
  set port-type data
  enable
create member-port Ethernet1/3
  exit
create member-port Ethernet1/4
  exit
exit
create port-channel 3
  set port-type data
  enable
create member-port Ethernet1/5
  exit
create member-port Ethernet1/6
  exit
exit
create port-channel 4
  set port-type mgmt
  enable
create member-port Ethernet2/1
  exit
create member-port Ethernet2/2
  exit
exit
create port-channel 48
  set port-type cluster
  enable
create member-port Ethernet2/3
  exit
exit
exit
commit-buffer

scope ssa
  enter logical-device ASA1 asa "1,2,3" clustered
  enter cluster-bootstrap
    set chassis-id 2
    set ipv4 gateway 10.1.1.254
    set ipv4 pool 10.1.1.11 10.1.1.15
    set ipv6 gateway 2001:DB8::AA
    set ipv6 pool 2001:DB8::11 2001:DB8::19
    set key
    Key: f@rscape
    set mode spanned-etherchannel
    set service-type cluster1
    set virtual ipv4 10.1.1.1 mask 255.255.255.0
    set virtual ipv6 2001:DB8::1 prefix-length 64
  exit
exit
commit-buffer
Add More Cluster Members

Add or replace an ASA cluster member.

Note

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

Before you begin

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

Procedure

To add another chassis to the cluster, repeat the procedure in *Create an ASA Cluster*, on page 125 except you must configure a unique *chassis-id*; otherwise, use the same configuration for the new chassis.

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.

```text
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:

```text
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
Delete a Logical Device

Procedure

Step 1  Enter security services mode:
Firepower# scope ssa

Step 2  View details for the logical devices on the chassis:
Firepower /ssa # show logical-device

Step 3  For each logical device that you want to delete, enter the following command:
Firepower /ssa # delete logical-device device_name

Step 4  View details for the applications installed on the logical devices:
Firepower /ssa # show app-instance

Step 5  For each application that you want to delete, enter the following commands:
a)  Firepower /ssa # scope slot slot_number
b)  Firepower /ssa/slot # delete app-instance application_name
c)  Firepower /ssa/slot # exit

Step 6  Commit the configuration:
commit-buffer

Commits the transaction to the system configuration.

Example

Firepower# scope ssa
Firepower /ssa # show logical-device

<table>
<thead>
<tr>
<th>Logical Device:</th>
<th>Name</th>
<th>Description</th>
<th>Slot ID</th>
<th>Mode</th>
<th>Operational State</th>
<th>Template Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTD</td>
<td></td>
<td></td>
<td>1,2,3</td>
<td>Clustered</td>
<td>Ok</td>
<td>ftd</td>
</tr>
</tbody>
</table>

Firepower /ssa # delete logical-device FTD
Firepower /ssa* # show app-instance

<table>
<thead>
<tr>
<th>Application Name</th>
<th>Slot ID</th>
<th>Admin State</th>
<th>Operational State</th>
<th>Running Version</th>
<th>Startup Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftd</td>
<td>1</td>
<td>Disabled</td>
<td>Stopping</td>
<td>6.0.0.837</td>
<td>6.0.0.837</td>
</tr>
</tbody>
</table>
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 132. For a cluster, connect to the primary unit. For a failover pair, connect to the active unit.

Step 2 Enter configuration mode:

```
enable
configure terminal
```

By default, the enable password is blank.

Step 3 Set the firewall mode to transparent:

```
firewall transparent
```

Step 4 Save the configuration:

```
write memory
```

For a cluster or failover pair, this configuration is replicated to secondary units:

```
asa(config)# firewall transparent
asa(config)# write memory
Building configuration...
Cryptochecksum: 9f831dfb 60dffa8c 1d939884 74735b69

3791 bytes copied in 0.160 secs
[OK]
asa(config)#
Beginning configuration replication to 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. For an inter-chassis cluster or for a failover pair, repeat steps 5 through 7 to redeploy the bootstrap configuration on each chassis.

Wait several minutes for the chassis/security modules to reload, and for the ASA to become operational again. The ASA now has an operational bootstrap configuration, but remains in transparent mode.

## Change an Interface on a Firepower Threat Defense Logical Device

You can allocate or unallocate an interface 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](page100) and [Add an EtherChannel (Port Channel)](page102).

- 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, you must use the Firepower Chassis Manager; the CLI does not support this change.

- 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**

Step 1 Enter security services mode:

```
Firepower# scope ssa
```

Step 2 Edit the logical device:
Firepower /ssa # scope logical-device device_name

Step 3 Unallocate an interface from the logical device:
Firepower /ssa/logical-device # delete external-port-link name
Enter the show external-port-link command to view interface names.

Step 4 Allocate a new interface to the logical device:
Firepower /ssa/logical-device* # create external-port-link name interface_id ftd

Step 5 Commit the configuration:
commit-buffer
Commits the transaction to the system configuration.

Step 6 Log into the Firepower Management Center.

Step 7 Select Devices > Device Management and click the edit icon (-pencil) for your FTD device. The Interfaces tab is selected by default.

Step 8 Click the Sync Interfaces from device button on the top left of the Interfaces tab.

Step 9 Click Save.
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 100 and Add an EtherChannel (Port Channel), on page 102.

- 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.

- 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

**Step 1** Enter security services mode:

```
Firepower# scope ssa
```

**Step 2** Edit the logical device:

```
Firepower /ssa# scope logical-device device_name
```

**Step 3** Unallocate an interface from the logical device:

```
Firepower /ssa/logical-device# delete external-port-link name
```

Enter the `show external-port-link` command to view interface names.

For a management interface, delete the current interface then commit your change using the `commit-buffer` command before you add the new management interface.

**Step 4** Allocate a new interface to the logical device:

```
Firepower /ssa/logical-device*# create external-port-link name interface_id asa
```

**Step 5** Commit the configuration:

```
commit-buffer
```

Commits the transaction to the system configuration.

---

Monitoring Logical Devices

- **show app**

  View available images.

  ```
  Firepower# scope ssa
  Firepower /ssa# show app
  Name | Version | Author | Supported Deploy Types | CSP Type | Is Default
  --------------- | --------------- | --------------- | --------------- | --------------- | ---------------
  app | 9.10.1 | cisco | Native | Application | Yes
  fttd | 6.2.3 | cisco | Native | Application | Yes
  ```

- **show app-instance**

  View the application instance status.

  ```
  Firepower# scope ssa
  Firepower /ssa# show app-instance
  App Name | Slot ID | Admin State | Oper State | Running Version | Startup Version
  --------------- | --------------- | --------------- | --------------- | --------------- | ---------------
  fttd | 1 | Enabled | Online | 6.2.1.62 | 6.2.1.62 | Not
  ```
Examples for Inter-Site Clustering

The following examples show supported cluster deployments.

**Spanned EtherChannel Transparent Mode North-South Inter-Site Example**

The following example shows 2 cluster members at each of 2 data centers placed between inside and outside routers (North-South insertion). The cluster members are connected by the cluster control link over the DCI. The cluster members at each site connect to the local switches using spanned EtherChannels for the inside and outside. Each EtherChannel is spanned across all chassis in the cluster.

The inside and outside routers at each data center use OSPF, which is passed through the transparent ASAs. Unlike MACs, router IPs are unique on all routers. By assigning a higher cost route across the DCI, traffic stays within each data center unless all cluster members at a given site go down. The lower cost route through the ASAs must traverse the same bridge group at each site for the cluster to maintain asymmetric connections. In the event of a failure of all cluster members at one site, traffic goes from each router over the DCI to the cluster members at the other site.

The implementation of the switches at each site can include:

- **Inter-site VSS/vPC**—In this scenario, you install one switch at Data Center 1, and the other at Data Center 2. One option is for the cluster units at each Data Center to only connect to the local switch, while the VSS/vPC traffic goes across the DCI. In this case, connections are for the most part kept local to each datacenter. You can optionally connect each unit to both switches across the DCI if the DCI can handle the extra traffic. In this case, traffic is distributed across the data centers, so it is essential for the DCI to be very robust.

- **Local VSS/vPC at each site**—For better switch redundancy, you can install 2 separate VSS/vPC pairs at each site. In this case, although the cluster units still have a spanned EtherChannel with Data Center 1 chassis connected only to both local switches, and Data Center 2 chassis connected to those local switches, the spanned EtherChannel is essentially “split.” Each local VSS/vPC sees the spanned EtherChannel as a site-local EtherChannel.
Spanned EtherChannel Transparent Mode East-West Inter-Site Example

The following example shows 2 cluster members at each of 2 data centers placed between the gateway router and two inside networks at each site, the App network and the DB network (East-West insertion). The cluster members are connected by the cluster control link over the DCI. The cluster members at each site connect to the local switches using spanned EtherChannels for both the App and DB networks on the inside and outside. Each EtherChannel is spanned across all chassis in the cluster.

The gateway router at each site uses an FHRP such as HSRP to provide the same destination virtual MAC and IP addresses at each site. A good practice to avoid unintended MAC address flapping is to statically add the gateway routers real MAC addresses to the ASA MAC address table using the `mac-address-table static outside_interface mac_address` command. Without these entries, if the gateway at site 1 communicates with the gateway at site 2, that traffic might pass through the ASA and attempt to reach site 2 from the inside interface and cause problems. The data VLANs are extended between the sites using Overlay Transport Virtualization (OTV) (or something similar). You must add filters to prevent traffic from traversing the DCI to the other site when the traffic is destined for the gateway router. If the gateway router at one site becomes unreachable, you must remove the filters so traffic can be sent to the other site’s gateway router.
See [Spanned EtherChannel Transparent Mode North-South Inter-Site Example](#), on page 139 for information about vPC/VSS options.

## History for Logical Devices

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inter-chassis clustering for 6 ASA modules</td>
<td>1.1.3</td>
<td>You can now enable inter-chassis clustering for the ASA. You can include up to 6 modules in up to 6 chassis.</td>
</tr>
<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. We introduced the following commands: enter cluster-bootstrap, enter logical-device clustered, set chassis-id, set ipv4 gateway, set ipv4 pool, set ipv6 gateway, set ipv6 pool, set key, set mode spanned-etherchannel, set port-type cluster, set service-type, set virtual ipv4, set virtual ipv6</td>
</tr>
</tbody>
</table>
CHAPTER 10

Configuration Import/Export

• About Configuration Import/Export, on page 143
• Exporting an FXOS Configuration File, on page 144
• Scheduling Automatic Configuration Export, on page 145
• Setting a Configuration Export Reminder, on page 147
• Importing a Configuration File, on page 148

About Configuration Import/Export

You can use the configuration export feature to export an XML file containing logical device and platform configuration settings for your Firepower 9300 chassis to a remote server. You can later import that configuration file to quickly apply the configuration settings to your Firepower 9300 chassis to return to a known good configuration or to recover from a system failure.

Guidelines and Restrictions

• Do not modify the contents of the configuration file. If a configuration file is modified, configuration import using that file might fail.

• Application-specific configuration settings are not contained in the configuration file. You must use the configuration backup tools provided by the application to manage application-specific settings and configurations.

• When you import a configuration to the Firepower 9300 chassis, all existing configuration on the Firepower 9300 chassis (including any logical devices) will be deleted and completely replaced by the configuration contained in the import file.

• We recommend that you only import a configuration file to the same Firepower 9300 chassis from which the configuration was exported.

• The platform software version of the Firepower 9300 chassis to which you are importing should be the same version as when the export was taken. If not, the import operation is not guaranteed to be successful. We recommend that you export a backup configuration whenever the Firepower 9300 chassis is upgraded or downgraded.

• The Firepower 9300 chassis to which you are importing must have the same Network Modules installed in the same slots as when the export was taken.
• The Firepower 9300 chassis to which you are importing must have the correct software application images installed for any logical devices defined in the export file that you are importing.

• To avoid overwriting existing backup files, please be sure to change the filename in the backup operation or copy the existing file to another location.

Exporting an FXOS Configuration File

Use the configuration export feature to export an XML file containing logical device and platform configuration settings for your Firepower 9300 chassis to a remote server.

Please review the About Configuration Import/Export for important information about using the configuration export feature.

Procedure

Step 1 To export a configuration file to a remote server:

```
scope system
export-config URL enabled
commit-buffer
```

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

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

**Note** You must specify the full path including filename. If you do not specify a filename, a hidden file is created in the specified path.

**Example:**

```
Firepower-chassis# scope system
Firepower-chassis /system # export-config scp://user1@192.168.1.2:/export/cfg-backup.xml enabled
Firepower-chassis /system/export-config # commit-buffer
```

Step 2 To check the status of the export task:

```
scope system
scope export-config hostname
show fsm status
```

**Example:**

```
Firepower-chassis# scope system
Firepower-chassis /system # scope export-config 192.168.1.2
Firepower-chassis /system/export-config # show fsm status
```
Hostname: 192.168.1.2

FSM 1:
Remote Result: Not Applicable
Remote Error Code: None
Remote Error Description:
Status: Nop
Previous Status: Backup Success
Timestamp: 2016-01-03T15:32:08.636
Try: 0
Progress (%): 100
Current Task:

Step 3  To view existing export tasks:
scope system
show export-config

Step 4  To modify an existing export task:
scope system
scope export-config hostname

Use the following commands to modify the export task:
  • {enable|disable}
  • set description <description>
  • set password <password>
  • set port <port>
  • set protocol {ftp|scp|sftp|tftp}
  • set remote-file path_and_filename
  • set user <user>

Step 5  To delete an export task:
scope system
delete export-config hostname
commit-buffer

Scheduling Automatic Configuration Export

Use the scheduled export feature to automatically export an XML file containing logical device and platform configuration settings for your Firepower 9300 chassis to a remote server. You can schedule the exports to be run daily, weekly, or every two weeks. The configuration export will be executed according to the schedule
based on the when the scheduled export feature is enabled. So, for example, if you enable weekly scheduled export on a Wednesday at 10:00pm, the system will trigger a new export every Wednesday at 10:00pm.

Please review the About Configuration Import/Export for important information about using the configuration export feature.

**Procedure**

To create a scheduled export task:

a) Set the scope to export policy configuration:

   ```
   scope org
   scope cfg-export-policy default
   ```

b) Enable the export policy:

   ```
   set adminstate enable
   ```

c) Specify the protocol to use when communicating with the remote server:

   ```
   set protocol {ftp|scp|sftp|tftp}
   ```

d) Specify the hostname or IP address of the location where the backup file should be stored. This can be a server, storage array, local drive, or any read/write media that the Firepower 9300 chassis can access through the network.

   If you use a hostname rather than an IP address, you must configure a DNS server.

   ```
   set hostname hostname
   ```

e) If you are using a non-default port, specify the port number:

   ```
   set port port
   ```

f) Specify the username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP:

   ```
   set user username
   ```

g) Specify the password for the remote server username. This field does not apply if the protocol is TFTP:

   ```
   set password password
   ```

h) Specify the full path to where you want the configuration file exported including the filename. If you omit the filename, the export procedure assigns a name to the file:

   ```
   set remote-file path_and_filename
   ```

i) Specify the schedule on which you would like to have the configuration automatically exported. This can be one of the following: Daily, Weekly, or BiWeekly:

   ```
   set schedule {daily|weekly|bi-weekly}
   ```

j) Commit the transaction to the system configuration:

   ```
   commit-buffer
   ```

**Example:**
Setting a Configuration Export Reminder

Use the Export Reminder feature to have the system generate a fault when a configuration export hasn't been executed in a certain number of days.

**Procedure**

To create a configuration export reminder:

```plaintext
scope org
scope config-export-reminder
set frequency days
set adminstate {enable|disable}
commit-buffer
```

**Example:**

```
Firepower-chassis# scope org
Firepower-chassis /org # scope config-export-reminder
Firepower-chassis /org/config-export-reminder # set frequency 10
Firepower-chassis /org/config-export-reminder* # set adminstate enable
Firepower-chassis /org/config-export-reminder* # commit-buffer
Firepower-chassis /org/config-export-reminder* # show detail
```

Config Export Reminder:
- Config Export Reminder (Days): 10
Importing a Configuration File

You can use the configuration import feature to apply configuration settings that were previously exported from your Firepower 9300 chassis. This feature allows you to return to a known good configuration or to recover from a system failure. Please review the About Configuration Import/Export for important information about using the configuration import feature.

Procedure

Step 1  To import a configuration file from a remote server:

```
scope system
import-config URL enabled
commit-buffer
```

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

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

Example:

```
Firepower-chassis# scope system
Firepower-chassis /system # import-config scp://user1@192.168.1.2:/import/cfg-backup.xml enabled
```

Warning: After configuration import any changes on the breakout port configuration will cause the system to reboot.

```
Firepower-chassis /system/import-config # commit-buffer
```

Step 2  To check the status of the import task:

```
scope system
scope import-config hostname
show fsm status
```

Example:

```
Firepower-chassis# scope system
Firepower-chassis /system # scope import-config 192.168.1.2
Firepower-chassis /system/import-config # show fsm status
```

Hostname: 192.168.1.2
FSM 1:
Remote Result: Not Applicable
Remote Error Code: None
Remote Error Description:
Status: Import Wait For Switch
Previous Status: Import Config Breakout
Timestamp: 2016-01-03T15:45:03.963
Try: 0
Progress (%): 97
Current Task: updating breakout port configuration(FSM-STAGE:sam:dme:
MgmtImporterImport:configBreakout)

**Step 3**  To view existing import tasks:

```bash
scope system
show import-config
```

**Step 4**  To modify an existing import task:

```bash
scope system
scope import-config hostname
```

Use the following commands to modify the import task:

- `{enable|disable}`
- `set description <description>`
- `set password <password>`
- `set port <port>`
- `set protocol {ftp|scp|sftp|tftp}`
- `set remote-file path_and_filename`
- `set user <user>`

**Step 5**  To delete an import task:

```bash
scope system
delete import-config hostname
commit-buffer
```
Packet Capture

The Packet Capture tool is a valuable asset for use in debugging connectivity and configuration issues and for understanding traffic flows through your Firepower 9300 chassis. You can use the Packet Capture tool to log traffic that is going through specific interfaces on your Firepower 9300 chassis.

You can create multiple packet capture sessions, and each session can capture traffic on multiple interfaces. For each interface included in a packet capture session, a separate packet capture (PCAP) file will be created.

Backplane Port Mappings

The Firepower 9300 chassis uses the following mappings for internal backplane ports:

<table>
<thead>
<tr>
<th>Security Module</th>
<th>Port Mapping</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Module 1/Security Engine</td>
<td>Ethernet1/9</td>
<td>Internal-Data0/0</td>
</tr>
<tr>
<td>Security Module 1/Security Engine</td>
<td>Ethernet1/10</td>
<td>Internal-Data0/1</td>
</tr>
<tr>
<td>Security Module 2</td>
<td>Ethernet1/11</td>
<td>Internal-Data0/0</td>
</tr>
<tr>
<td>Security Module 2</td>
<td>Ethernet1/12</td>
<td>Internal-Data0/1</td>
</tr>
<tr>
<td>Security Module 3</td>
<td>Ethernet1/13</td>
<td>Internal-Data0/0</td>
</tr>
<tr>
<td>Security Module 3</td>
<td>Ethernet1/14</td>
<td>Internal-Data0/1</td>
</tr>
</tbody>
</table>
Guidelines and Limitations for Packet Capture

The Packet Capture tool has the following limitations:

- Can capture only up to 100 Mbps.
- Packet capture sessions can be created even when there is not enough storage space available to run the packet capture session. You should verify that you have enough storage space available before you start a packet capture session.
- Does not support multiple active packet capturing sessions.
- There is no option to filter based on source or destination IPv6 address.
- Captures only at the ingress stage of the internal switch.
- Filters are not effective on packets that cannot be understood by the internal switch (for example Security Group Tag and Network Service Header packets).
- You cannot capture packets for an EtherChannel as a whole. However, for an EtherChannel allocated to a logical device, you can capture packets on each member interface of the EtherChannel.
- You cannot copy or export a PCAP file while the capture session is still active.
- When you delete a packet capture session, all packet capture files associated with that session are also deleted.

Creating or Editing a Packet Capture Session

**Procedure**

**Step 1** Enter packet capture mode:

```
Firepower-chassis # scope packet-capture
```

**Step 2** Create a filter; see Configuring Filters for Packet Capture, on page 154.

You can apply filters to any of the interfaces included in a packet capture session.

**Step 3** To create or edit a packet capture session:

```
Firepower-chassis/packet-capture # enter session session_name
```

**Step 4** Specify the buffer size to use for this packet capture session:

```
Firepower-chassis/packet-capture/session* # set session-memory-usage session_size_in_megabytes
```

The specified buffer size must be between 256 and 2048 MB.

**Step 5** Specify the physical source ports that should be included in this packet capture session.

You can capture from multiple ports and can capture from both physical ports and application ports during the same packet capture session. A separate packet capture file is created for each port included in the session.
You cannot capture packets for an EtherChannel as a whole. However, for an EtherChannel allocated to a logical device, you can capture packets on each member interface of the EtherChannel.

**Note** To remove a port from the packet capture session, use `delete` instead of `create` in the commands listed below.

a) Specify the physical port.

```
Firepower-chassis /packet-capture/session* # create {phy-port | phy-aggr-port} port_id
```

**Example:**

```
Firepower-chassis /packet-capture/session* # create phy-port Ethernet1/1
Firepower-chassis /packet-capture/session/phy-port* #
```

b) (Optional) Apply the desired filter.

```
Firepower-chassis /packet-capture/session/phy-port* # set {source-filter} filtername
```

**Note** To remove a filter from a port, use `set source-filter ""`.

c) Repeat the steps above as needed to add all desired ports.

**Step 6**

Specify the application source ports that should be included in this packet capture session.

You can capture from multiple ports and can capture from both physical ports and application ports during the same packet capture session. A separate packet capture file is created for each port included in the session.

**Note** To remove a port from the packet capture session, use `delete` instead of `create` in the commands listed below.

a) Specify the application port.

```
Firepower-chassis /packet-capture/session* # create app_port module_slot link_name interface_name app_name
```

b) (Optional) Apply the desired filter.

```
Firepower-chassis /packet-capture/session/phy-port* # set {source-filter} filtername
```

**Note** To remove a filter from a port, use `set source-filter ""`.

c) Repeat the steps above as needed to add all desired application ports.

**Step 7**

If you want to start the packet capture session now:

```
Firepower-chassis /packet-capture/session* # enable
```

Newly created packet-capture sessions are disabled by default. Explicit enabling of a session activates the packet capture session when the changes are committed. If another session is already active, enabling a session will generate an error. You must disable the already active packet-capture session before you can enable this session.

**Step 8**

Commit the transaction to the system configuration:

```
Firepower-chassis /packet-capture/session* # commit-buffer
```

Cisco Firepower 9300 FXOS CLI Configuration Guide, 1.1(3)
If you enabled the packet capture session, the system will begin capturing packets. You will need to stop capturing before you can download the PCAP files from your session.

---

**Example**

```
Firepower-chassis# scope packet-capture
Firepower-chassis packet-capture # create session asa1inside
Firepower-chassis packet-capture/session # set session-memory-usage 256
Firepower-chassis packet-capture/session* # create phy-port Ethernet3/1
Firepower-chassis packet-capture/session* # create phy-aggr-port Ethernet2/1/1
Firepower-chassis packet-capture/session* # create app-port 1 link1 Ethernet 1/1 asa
Firepower-chassis packet-capture/session* # create filter interfacevlan100
Firepower-chassis packet-capture/session* # set ivlan 100
Firepower-chassis packet-capture/session* # set srcIP 6.6.6.6
Firepower-chassis packet-capture/session* # set srcPort 80
Firepower-chassis packet-capture/session* # set destIP 10.10.10.10
Firepower-chassis packet-capture/session* # set destPort 5050
Firepower-chassis packet-capture/session* # exit
Firepower-chassis packet-capture/session* # scope phy-port Ethernet3/1
Firepower-chassis packet-capture/session/phy-port* # set src-filter interfacevlan100
Firepower-chassis packet-capture/session/PHY-port* # exit
Firepower-chassis packet-capture/session* # scope app-port 1 link1 Ethernet1/1 asa
Firepower-chassis packet-capture/session/app-port* # set src-filter interfacevlan100
Firepower-chassis packet-capture/session/app-port* # exit
Firepower-chassis packet-capture/session* # enable
Firepower-chassis packet-capture/session* # commit-buffer
Firepower-chassis packet-capture/session #
```

**Configuring Filters for Packet Capture**

You can create filters to limit the traffic that is included in a packet capture session. You can select which interfaces should use a specific filter while creating a packet capture session.

---

**Note**

If you modify or delete a filter that is applied to a packet capture session that is currently running, the changes will not take affect until you disable that session and then reenable it.

---

**Procedure**

**Step 1**

Enter packet capture mode:

```
Firepower-chassis # scope packet-capture
```

**Step 2**

To create a new packet capture filter:

```
Firepower-chassis /packet-capture # create filter filter_name
```

To edit an existing packet capture filter:

```
Firepower-chassis /packet-capture # enter filter filter_name
```
To delete an existing packet capture filter:
Firepower-chassis/packet-capture # delete filter filter_name

Step 3
Specify the filter details by setting one or more filter properties:
Firepower-chassis/packet-capture/filter* # set <filterprop filterprop_value

Table 5: Supported Filter Properties

<table>
<thead>
<tr>
<th>Filter Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ivlan</td>
<td>Inner VLAN ID (vlan of packet while ingressing port)</td>
</tr>
<tr>
<td>ovlan</td>
<td>Outer VLAN ID (vlan added by the Firepower 9300 chassis)</td>
</tr>
<tr>
<td>srcip</td>
<td>Source IP Address (IPv4)</td>
</tr>
<tr>
<td>destip</td>
<td>Destination IP Address (IPv4)</td>
</tr>
<tr>
<td>srcport</td>
<td>Source Port Number</td>
</tr>
<tr>
<td>destport</td>
<td>Destination Port Number</td>
</tr>
<tr>
<td>protocol</td>
<td>IP Protocol [IANA defined Protocol values in decimal format]</td>
</tr>
<tr>
<td>ethertype</td>
<td>Ethernet Protocol type [IANA defined Ethernet Protocol type value in decimal format. For eg: IPv4 = 2048, IPv6 = 34525, ARP = 2054, SGT = 35081]</td>
</tr>
<tr>
<td>srcmac</td>
<td>Source Mac Address</td>
</tr>
<tr>
<td>destmac</td>
<td>Destination Mac Address</td>
</tr>
</tbody>
</table>

Example
Firepower-chassis# scope packet-capture
Firepower-chassis packet-capture # create filter interface1vlan100
Firepower-chassis packet-capture/filter* # set ivlan 100
Firepower-chassis packet-capture/filter* # set srcip 6.6.6.6
Firepower-chassis packet-capture/filter* # set srcport 80
Firepower-chassis packet-capture/filter* # set destip 10.10.10.10
Firepower-chassis packet-capture/filter* # set destport 5050
Firepower-chassis packet-capture/filter* # commit-buffer

Starting and Stopping a Packet Capture Session

Procedure

Step 1
Enter packet capture mode:
Firepower-chassis # scope packet-capture
Step 2  Enter the scope for the packet capture session that you want to start or stop:
Firepower-chassis /packet-capture # enter session session_name

Step 3  To start a packet capture session:
Firepower-chassis /packet-capture/session* # enable [append | overwrite]

Note  You cannot start a packet capture session while another session is running.

While the packet capture session is running, the file size for the individual PCAP files will increase as traffic is captured. Once the Buffer Size limit is reached, the system will start dropping packets and you will see the Drop Count field increase.

Step 4  To stop a packet capture session:
Firepower-chassis /packet-capture/session* # disable

Step 5  Commit the transaction to the system configuration:
Firepower-chassis /packet-capture/session* # commit-buffer

If you enabled the packet capture session, the PCAP files for the interfaces included in the session will start collecting traffic. If the session is configured to overwrite session data, the existing PCAP data will be erased. If not, data will be appended to the existing file (if any).

Example
Firepower-chassis# scope packet-capture
Firepower-chassis packet-capture # scope session asalinside
Firepower-chassis packet-capture/session # enable append
Firepower-chassis packet-capture/session* # commit-buffer
Firepower-chassis packet-capture/session #

---

Downloading a Packet Capture File

You can download the Packet Capture (PCAP) files from a session to your local computer so that they can be analyzed using a network packet analyzer.

PCAP files are stored into the workspace://packet-capture directory and use the following naming conventions:
workspace://packet-capture/session-<id>/<session-name>-<interface-name>.pcap

Procedure

To copy a PCAP file from the Firepower 9300 chassis:

Note  You should stop the packet capture session before you download the PCAP files from that session.

a)  Connect to local management:
Firepower-chassis # connect localmgmt

b) Copy the PCAP files:

    # copy pcap_file copy_destination

---

Example

Firepower-chassis# connect localmgmt

    # copy workspace:/packet-capture/session-1/test-ethernet-1-1-0.pcap
    scp://user@10.10.10.1:/workspace/
## INDEX

### A

| AAA | 85, 86, 89, 90, 91, 92, 93, 94 |
| LDAP providers | 85, 86, 89 |
| RADIUS providers | 89, 90, 91 |
| TACACS+ providers | 92, 93, 94 |

accessing the command line interface 12

accounts 30, 36, 37, 38, 42

locally authenticated 30, 36, 37, 38, 42

asa 49, 112, 115, 125, 132, 134

connecting to 132

creating a cluster 125

creating a clustered 112

creating a standalone asa logical device 115

deleting a logical device 134

exiting from connection 132

updating image version 49

asa images 43, 44, 47

about 43

downloading from Cisco.com 44

downloading to the Firepower security appliance 47

authentication 31

default 31

authNoPriv 64

authPriv 64

### B

breakout cables 104

configuring 104

breakout ports 104

### C

call home 19

configure http proxy 19

certificate 72

about 72

chassis 9

initial configuration 9

Cisco Secure Package 43, 44, 47

about 43

downloading from Cisco.com 44

downloading to the Firepower security appliance 47

cli, See command line interface

CLI session limits 7

clustering 110, 112, 113, 122, 123

cluster control link 122

redundancy 122

size 122

device-local EtherChannels, configuring on switch 113

management 123

network 123

member requirements 110

software requirements 110

spanning-tree portfast 112

upgrading software 110

clusters 112, 121, 125

about 121

creating 112, 125

command line interface 12

accessing 12

command modes 3

commands 6

history 6

communication services 66, 72, 73, 74, 75, 77, 78

HTTPS 72, 73, 74, 75, 77, 78

SNMP 66

community, SNMP 66

configuration import/export 143

guidelines 143

restrictions 143

configuring 72, 73, 74, 75, 77, 78

HTTPS 72, 73, 74, 75, 77, 78

connecting to a logical device 132

console 33

timeout 33

creating packet capture session 152

CSP, See Cisco Secure Package

### D

date 61

setting manually 61

date and time 57

configuring 57

DNS 97

downloading packet capture file 156
INDEX

E
enabling 66
   SNMP 66
enforcing password strength 34
exiting from logical device connection 132
export configuration 143

F
Firepower chassis 9
   initial configuration 9
Firepower eXtensible OS 46
   upgrading the platform bundle 46
Firepower platform bundle 43, 44, 45, 46
   about 43
   downloading from Cisco.com 44
   downloading to the Firepower security appliance 44
   upgrading 46
   verifying integrity 45
Firepower security appliance 1
   overview 1
firmware 50
   upgrading 50
fpga 50
   upgrading 50

H
high-level task list 9
history, passwords 30
http proxy 19
   configuring 19
HTTPS 33, 72, 73, 74, 75, 77, 78, 81, 83
   certificate request 74, 75
   changing port 81
   configuring 79
   creating key ring 72
   disabling 83
   importing certificate 78
   regenerating key ring 73
   timeout 33
   trusted point 77

I
image version 49
   updating 49
images 43, 44, 45, 46, 47
   downloading from Cisco.com 44
   downloading to the Firepower security appliance 44, 47
   managing 43
   upgrading the Firepower eXtensible Operating System platform bundle 46
   verifying integrity 45
import configuration 143
informs 64
   about 64
initial configuration 9
interfaces 100
   configuring 100
   properties 100

K
key ring 72, 73, 74, 75, 77, 78, 82
   about 72
   certificate request 74, 75
   creating 72
   deleting 82
   importing certificate 78
   regenerating 73
   trusted point 77

L
LDAP 85, 86, 89
LDAP providers 86, 89
   creating 86
   deleting 89
license 20
   registering 20
license authority 20
locally authenticated users 30, 36, 37, 38, 42
   change interval 36
   clearing password history 42
   no change interval 37
   password history count 38
   password profile 30
logical devices 49, 112, 115, 125, 132, 134
   connecting to 132
   creating a cluster 112, 125
   creating a standalone 115
   deleting 134
   exiting from connection 132
   updating image version 49

M
managed objects 3
management IP address 55
   changing 55

N
noAuthNoPriv 64
NTP 57, 59, 60
   adding 59
   configuring 57, 59
   deleting 60
O

object commands 5

P

packet capture 151, 152, 154, 155, 156
  creating packet capture session 152
  downloading PCAP file 156
  filter 154
  starting a packet capture session 155
  stopping a packet capture session 155
password profile 30, 36, 37, 38, 42
  about 30
  change interval 36
  clearing password history 42
  no change interval 37
  password history count 38
passwords 27, 30, 31, 34
  change interval 31
  guidelines 27
  history count 30
  strength check 34
PCAP, See packet capture
PCAP file 156
  downloading 156
pending commands 6
PKI 72
platform bundle 43, 44, 45, 46
  about 43
  downloading from Cisco.com 44
  downloading to the Firepower security appliance 44
  upgrading 46
  verifying integrity 45
policies 33
  role for remote users 33
port channels 102
  configuring 102
profiles 30
  password 30

R

RADIUS 89, 90, 91
RADIUS providers 90, 91
  creating 90
  deleting 91
registering a license 20
role policy for remote users 33
rommon 50
  upgrading 50
RSA 72

S

session timeout 33
smart call home 19
  configure http proxy 19
SNMP 63, 64, 65, 66, 67, 69, 71
  about 63
  community 66
  enabling 66
  notifications 64
  privileges 64
  security levels 64
  support 63, 65
  traps 67, 69
    creating 67
    deleting 69
  users 69, 71
    creating 69
    deleting 71
  Version 3 security features 65
SNMPv3 65
  security features 65
SSH 33, 62
  configuring 62
  timeout 33
syslog 94
  configuring local destinations 94
  configuring local sources 94
  configuring remote destinations 94
system 9
  initial configuration 9

T

TACACS+ 92, 93, 94
TACACS+ providers 93, 94
  creating 93
  deleting 94
task flow 9
Telnet 33, 62
  configuring 62
  timeout 33
threat defense images 47
  downloading to the Firepower security appliance 47
time 61
  setting manually 61
time zone 57, 59, 61
  setting 57, 59, 61
timeout 33
  console 33
  HTTPS, SSH, and Telnet 33
traps 64, 67, 69
  about 64
  creating 67
  deleting 69
trusted points 72, 77, 82
   about 72
   creating 77
   deleting 82

U

upgrading the firmware 50
user accounts 30, 36, 37, 38, 42
password profile 30, 36, 37, 38, 42
users 7, 25, 26, 27, 30, 31, 33, 34, 36, 37, 38, 41, 42, 69, 71
   activating 41
   CLI session limits 7

users (continued)
   creating 38
   deactivating 41
   default authentication 31
   deleting 41
   locally authenticated 30, 36, 37, 38, 42
   managing 25
   naming guidelines 26
   password guidelines 27
   password strength check 34
   remote, role policy 33
   roles 30
   SNMP 69, 71