CHAPTER 1

Firepower 4100 Chassis Initial Configuration

Is This Chapter for You?
This chapter describes how to perform the initial setup for the Cisco Firepower 4100 chassis, including configuring interfaces for use with the ASA and Firepower Threat Defense (FTD) logical devices.

- Is This Guide for You?, on page 1
- About the Firepower 4100 Chassis, on page 2
- End-to-End Procedure, on page 3
- Cable the Chassis, on page 5
- Perform Initial Chassis Setup, on page 7
- Log Into the Firepower Chassis Manager, on page 10
- Configure NTP, on page 10
- Add FXOS Users, on page 12
- Configure Interfaces, on page 14
- Upload Software Images to the Chassis, on page 19
- History for FXOS, on page 21

Is This Guide for You?
This guide describes how to set up the Firepower 4100 chassis for use with the ASA and/or FTD application. This guide describes the following deployments:

- Standalone ASA using ASDM
- Standalone FTD using the Firepower Device Manager (FDM)
- Standalone FTD as either a native or container instance (multi-instance capability) using the Firepower Management Center (FMC)

This guide does not cover the following deployments, for which you should refer to the FXOS, ASA, FDM, and FMC configuration guides:

- High Availability/Failover
- Clustering
- Radware DefensePro decorator application
- CLI configuration
This guide also walks you through configuring a basic security policy; if you have more advanced requirements, refer to the configuration guide.

**About the Firepower 4100 Chassis**

The Cisco Firepower 4100 chassis is a next-generation platform for network and content security solutions. The Firepower 4100 includes a supervisor and a single security engine, on which you can install logical devices. It also accepts multiple high performance network modules.

**How the Logical Device Works with the Firepower 4100**

The Firepower 4100 runs its own operating system on the supervisor called the Firepower eXtensible Operating System (FXOS). The on-the-box Firepower Chassis Manager provides simple, GUI-based management capabilities. You configure hardware interface settings, smart licensing (for the ASA), and other basic operating parameters on the supervisor using the Firepower Chassis Manager. To use the FXOS CLI, see the FXOS CLI configuration guide.

A logical device lets you run one application instance and also one optional decorator application to form a service chain. When you deploy the logical device, the supervisor downloads an application image of your choice and establishes a default configuration. You can then configure the security policy within the application operating system.

Logical devices cannot form a service chain with each other, and they cannot communicate over the backplane with each other. All traffic must exit the chassis on one interface and return on another interface to reach another logical device. For container instances, you can share data interfaces; only in this case can multiple logical devices communicate over the backplane.

**Supported Applications**

You can deploy logical devices on your chassis using the following application types.

**Firepower Threat Defense**

The FTD provides next-generation firewall services, including stateful firewalls, routing, VPN, Next-Generation Intrusion Prevention System (NGIPS), Application Visibility and Control (AVC), URL filtering, and Advanced Malware Protection (AMP).

You can manage the FTD using one of the following managers:

- FMC—A full-featured, multidevice manager on a separate server.
- Firepower Device Manager (FDM)—A simplified, single device manager included on the device.

**ASA**

The ASA provides advanced stateful firewall and VPN concentrator functionality in one device. You can manage the ASA using one of the following managers:

- ASDM—A single device manager included on the device. This guide describes how to manage the ASA using ASDM.
- CLI
• Cisco Security Manager—A multidevice manager on a separate server.

Radware DefensePro (Decorator)
You can install Radware DefensePro (vDP) to run in front of the ASA or FTD as a decorator application. vDP is a KVM-based virtual platform that provides distributed denial-of-service (DDoS) detection and mitigation capabilities on the Firepower 4100. Traffic from the network must first pass through the vDP before reaching the ASA or FTD.

To deploy vDP, see the FXOS configuration guide.

Logical Device Application Instances: Container or Native

Logical device application instances run in the following deployment types:

• Native instance—A native instance uses all of the resources (CPU, RAM, and disk space) of the security engine, so you can only install one native instance.

• Container instance—A container instance uses a subset of resources of the security engine, so you can install multiple container instances. Note: Multi-instance capability is only supported for the FTD; it is not supported for the ASA or in conjunction with vDP.

Maximum Container Instances per Model

• Firepower 4110—3
• Firepower 4120—3
• Firepower 4140—7
• Firepower 4150—7

End-to-End Procedure

See the following tasks to set up the Firepower 4100 chassis, and to deploy logical devices on your chassis.
<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Pre-Configuration: Set up Firepower 4100 hardware. See the Firepower 4100 hardware guide.</td>
</tr>
<tr>
<td>2</td>
<td>Pre-Configuration: Cable the Chassis, on page 5.</td>
</tr>
<tr>
<td>3</td>
<td>FXOS Console CLI: Perform Initial Chassis Setup, on page 7.</td>
</tr>
<tr>
<td>4</td>
<td>Firepower Chassis Manager: Log Into the Firepower Chassis Manager, on page 10.</td>
</tr>
<tr>
<td>5</td>
<td>Firepower Chassis Manager: Configure NTP, on page 10.</td>
</tr>
<tr>
<td>6</td>
<td>Firepower Chassis Manager: Add FXOS Users, on page 12.</td>
</tr>
<tr>
<td>7</td>
<td>Firepower Chassis Manager: Configure Interfaces, on page 14.</td>
</tr>
<tr>
<td>8</td>
<td>Create a logical device (see application chapters)</td>
</tr>
<tr>
<td>9</td>
<td>Complete application configuration</td>
</tr>
</tbody>
</table>
### Cable the Chassis

Cable the following interfaces for initial chassis setup, continued monitoring, and logical device use.

- **Console port**—Connect your management computer to the console port to perform initial setup of the chassis. The Firepower 4100 includes an RS-232–to–RJ-45 serial console cable. You might need to use a third party serial-to-USB cable to make the connection.

- **Chassis Management port**—Connect the chassis management port to your management network for configuration and ongoing chassis management.

- **Logical device Management interface**—Use one or more interfaces to manage the logical devices. You can choose any interfaces on the chassis for this purpose other than the chassis management port, which is reserved for FXOS management. For multi-instance support, Management interfaces can be shared among logical devices, or you can use a separate interface per logical device. Typically, you share a management interface with all logical devices, or if you use separate interfaces, put them on a single management network. But your exact network requirements may vary.

- **Data interfaces**—Connect the data interfaces to your logical device data networks. You can configure physical interfaces, EtherChannels, VLAN subinterfaces (for container instances only), and breakout ports to divide up high-capacity interfaces. For multi-instance support, you can cable multiple logical devices to the same networks or to different networks, as your network needs dictate. For container instances, you can share data interfaces; only in this case can multiple logical devices communicate over the backplane. Otherwise, all traffic must exit the chassis on one interface and return on another interface to reach another logical device. For details about shared interface limitations and guidelines, see the FXOS configuration guide.
All interfaces other than the console port require SFP/SFP+/QSFP transceivers. See the hardware installation guide for supported transceivers.

Although not covered in this guide, for High Availability, use a Data interface for the failover/state link. For inter-chassis clustering, use an EtherChannel that is defined on the chassis as a Cluster type interface.

**FTD with FMC Cabling**

Place the FMC on (or accessible from) the logical device management network. Note that the FTD and FMC need access to the internet via the Management network for updates.

When planning your connectivity, keep in mind that the FTD Management interface is shared between the following logical interfaces:

- Management logical interface—This management plane interface communicates with the FMC, downloads updates, and provides SSH access to the FTD CLI.

- Diagnostic logical interface—This data plane interface is listed with other data interfaces in the FMC. As a management-only interface that does not allow through traffic, this interface is useful for syslog or SNMP, but it is not required for use.

The above cabling example connects the management network to the FTD inside network (or any interface with internet access) so that the FTD acts as the internet gateway. You can either connect the FTD Management interface and other management devices to the inside interface directly (using a switch), or you can put a router between the management network and the FTD inside network.

In the direct-connect scenario, it's important that you do not configure an IP address for the Diagnostic logical interface in the FMC. Because the FTD Management logical interface is not a regular interface and does not participate in FTD routing, you can directly-connect it to an FTD data network as shown. But if you assign an IP address to the Diagnostic interface, it cannot be on the same network as other data interfaces. In that case, you would need to route between Management/Diagnostic and another FTD interface.
FTD with FDM Cabling

Perform initial FTD configuration on the logical device Management interface. You can later enable management from any data interface. The FTD requires internet access for licensing and updates, and the default behavior is to route management traffic to the gateway IP address you specified when you deployed the FTD. If you want to route management traffic over the backplane to the data interfaces instead, you can configure that setting in FDM later.

ASA Cabling

Perform initial ASA configuration on the Management interface. You can later enable management from any data interface.

Perform Initial Chassis Setup

The first time you access the FXOS CLI at the console, a setup wizard prompts you for the basic network configuration so you can access the Firepower Chassis Manager (using HTTPS) or the FXOS CLI (using SSH) from the chassis management port.

Note

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

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

Gather the following information for use with the setup script:

- New admin password
- Management IP address and subnet mask
- Gateway IP address
- Subnets from which you want to allow HTTPS and SSH access
- Hostname and domain name
- DNS server IP address

Procedure

Step 1  Power on the chassis.

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

The Firepower 4100 includes an RS-232–to–RJ-45 serial console cable. You might need to use a third party
serial-to-USB cable to make the connection. Use the following serial parameters:

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

Step 3  When prompted, log in with the username admin and the password cisco123.

Step 4  Complete the system configuration as prompted.

Example:

---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of the system. Only minimal configuration including IP connectivity to the FXOS Supervisor is performed through these steps.

Type Ctrl-C at any time for more options or to abort configuration and reboot system.
To back track or make modifications to already entered values, complete input till end of section and answer no when prompted to apply configuration.

You have chosen to setup a new Security Appliance.
Continue? (yes/no): y

Enforce strong password? (yes/no) [y]: n

Enter the password for "admin": Farscape432
Confirm the password for "admin": Farscape432
Enter the system name: firepower-9300
Supervisor Mgmt IP address : 10.80.6.12
Supervisor Mgmt IPv4 netmask : 255.255.255.0
IPv4 address of the default gateway : 10.80.6.1

The system cannot be accessed via SSH if SSH Mgmt Access is not configured.

Do you want to configure SSH Mgmt Access? (yes/no) [y]: y

SSH Mgmt Access host/network address (IPv4/IPv6): 10.0.0.0
SSH Mgmt Access IPv4 netmask: 255.0.0.0

Firepower Chassis Manager cannot be accessed if HTTPS Mgmt Access is not configured.

Do you want to configure HTTPS Mgmt Access? (yes/no) [y]: y

HTTPS Mgmt Access host/network address (IPv4/IPv6): 10.0.0.0
HTTPS Mgmt Access IPv4 netmask: 255.0.0.0

Configure the DNS Server IP address? (yes/no) [n]: y

DNS IP address : 10.164.47.13

Configure the default domain name? (yes/no) [n]: y

Default domain name : cisco.com

Following configurations will be applied:

Switch Fabric=A
System Name=firepower-9300
Enforced Strong Password=no
Supervisor Mgmt IP Address=10.89.5.14
Supervisor Mgmt IP Netmask=255.255.255.192
Default Gateway=10.89.5.1
SSH Access Configured=yes
  SSH IP Address=10.0.0.0
  SSH IP Netmask=255.0.0.0
HTTPS Access Configured=yes
  HTTPS IP Address=10.0.0.0
  HTTPS IP Netmask=255.0.0.0
DNS Server=72.163.47.11
Domain Name=cisco.com

Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): y

Applying configuration. Please wait... Configuration file – Ok

.......

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

[...]

firepower-chassis#
Log Into the Firepower Chassis Manager

Use the Firepower Chassis Manager to configure chassis settings, including enabling interfaces and deploying logical devices.

**Before you begin**

- You can only access the Firepower Chassis Manager from a management computer with an IP address in the range you specified during the initial chassis setup.

**Procedure**

**Step 1**

Using a supported browser, enter the following URL.

`https://chassis_mgmt_ip_address`

- `chassis_mgmt_ip_address`—Identifies the IP address or hostname of the chassis management port that you entered during initial configuration.

**Step 2**

Enter the username `admin` and new password.

You can add more users later according to Add FXOS Users, on page 12.

**Step 3**

Click Login.

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

Configure NTP

Although you can set the time manually, we recommend that you use an NTP server. The correct time is required for Smart Software Licensing for the ASA and for FTD with FDM. For the FTD with FMC, the time must match between the chassis and the FMC. In this case, we recommend that you use the same NTP server on the chassis as on the FMC. Do not use the FMC itself as the NTP server; this method is not supported.

**Before you begin**

If you use a hostname for the NTP server, you must configure a DNS server if you did not already do so in the initial setup. See Platform Settings > DNS.
Procedure

**Step 1**
Choose *Platform Settings > NTP*.
The *Time Synchronization* page is selected by default.

**Step 2**
Click the *Use NTP Server* radio button.

**Step 3**
(Optional) Check the *NTP Server Authentication: Enable* check box if you need to authenticate the NTP server.

You are prompted to enable NTP authentication. Click *Yes* to require an authentication key ID and value for all NTP server entries.

Only SHA1 is supported for NTP server authentication.

**Step 4**
Click *Add*, and set the following parameters:

- **NTP Server**—The IP address or hostname of the NTP server.
- **Authentication Key** and **Authentication Value**—Obtain the key ID and value from the NTP server. For example, to generate the SHA1 key on NTP server Version 4.2.8p8 or later with OpenSSL installed, enter the `ntp-keygen -M` command, and then view the key ID and value in the ntp.keys file. The key is used to tell both the client and server which value to use when computing the message digest.

**Step 5**
Click *Add* to add the server.

You can add up to 4 NTP servers.

**Step 6**
Click *Save* to save the servers.

**Step 7**
Click *Current Time*, and from the *Time Zone* drop-down list, choose the appropriate time zone for the chassis.
Step 8  Click Save.

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

---

## Add FXOS Users

Add local users for Firepower Chassis Manager and FXOS CLI logins.

**Procedure**

### Step 1  Choose System > User Management.

### Step 2  Click Local Users.

### Step 3  Click Add User to open the Add User dialog box.
Step 4

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

- **User Name**—Sets the username, up to 32 characters. After you save the user, the login ID cannot be changed. You must delete the user account and create a new one.

- (Optional) **First Name**—Sets the first name of the user, up to 32 characters.

- (Optional) **Last Name**—Sets the last name of the user, up to 32 characters.

- (Optional) **Email**—Sets the email address for the user.

- (Optional) **Phone Number**—Sets the telephone number for the user.

- **Password** and **Confirm Password**—Sets the password associated with this account. If you enable the password strength check, then the password must be strong, and FXOS rejects any password that does not meet the strength check requirements. See the FXOS configuration guide for strong password guidelines.

- **Account Status**—Sets the status to **Active** or **Inactive**.

- **User Role**—Sets the role that represents the privileges you want to assign to the user account. All users are assigned the **Read-Only** role by default, and this role cannot be deselected. To assign a different role, click the role name in the window so that it is highlighted. You can use one of the following user roles:
Configure Interfaces

By default, physical interfaces are disabled. In FXOS, you can enable interfaces, add EtherChannels, add VLAN subinterfaces, and edit interface properties. To use an interface, you must physically enable it in FXOS, and then logically enable it in the application.

To configure breakout ports, see the FXOS configuration guide.

Interface Types

Each interface is one of the following types:

- **Data**—Use for regular data. Data interfaces cannot be shared between logical devices, and logical devices cannot communicate over the backplane to other logical devices. For traffic on Data interfaces, all traffic must exit the chassis on one interface and return on another interface to reach another logical device.

- **Data-sharing**—Use for regular data. Only supported with container instances (see Logical Device Application Instances: Container or Native, on page 3), these data interfaces can be shared by one or more container instances (FTD-using-FMC-only). Each container instance can communicate over the backplane with all other instances that share this interface. Shared interfaces can affect the number of container instances you can deploy. See the FXOS configuration guide for detailed information about using shared interfaces. Shared interfaces are not supported for bridge group member interfaces (in transparent mode or routed mode), inline sets, passive interfaces, or failover links.

- **Management (Mgmt)**—Use to manage application instances. A Management interface 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. This interface is separate from the chassis management port.

- **Admin**—Complete read-and-write access to the entire system.

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

- **Operations**—Read-and-write access to NTP configuration, Smart Call Home configuration for Smart Licensing, and system logs, including syslog servers and faults. Read access to the rest of the system.

- **AAA Administrator**—Read-and-write access to users, roles, and AAA configuration. Read access to the rest of the system.

- (Optional) **Account Expires**—Sets that this account expires. The account cannot be used after the date specified in the Expiry Date field. 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. By default, user accounts do not expire.

- (Optional) **Expiry Date**—The date on which the account expires. The date should be in the format yyyy-mm-dd. Click the calendar icon at the end of this field to view a calendar that you can use to select the expiration date.

**Step 5**  
Click Add.
• Firepower-eventing—Use as a secondary management interface for FTD devices when using FMC. To use this interface, you must configure its IP address and other parameters at the FTD CLI. See the FMC configuration guide for more information.

• Cluster—Use as the cluster control link for a clustered logical device. By default, the cluster control link is automatically created on Port-channel 48. See the FXOS configuration guide for more information. FDM does not support clustering.

You must configure a Management interface and at least one Data (or Data-sharing) interface before you deploy a logical device.

## Configure a Physical Interface

You can physically enable and disable interfaces, as well as set the interface speed and duplex. To use an interface, you must physically enable it in FXOS, and then logically enable it 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 an interface to the EtherChannel.

### Procedure

1. **Step 1** Click **Interfaces**.
   - The **All Interfaces** page shows a visual representation of the currently-installed interfaces at the top of the page and provides a listing of the installed interfaces in the table below.

2. **Step 2** Click the edit icon (.TextEdit) for the interface you want to edit to open the **Edit Interface** dialog box.

3. **Step 3** Check the **Enable** check box.

4. **Step 4** Choose the interface **Type**: Data, Data-sharing, Mgmt, or Firepower-eventing.

   ![Edit Interface - Ethernet1/1](image)

   **Note** There are limitations when using Data-sharing type interfaces; see the FXOS configuration guide for more information.

   For Firepower-eventing, see the FMC configuration guide.

5. **Step 5** (Optional) Choose the **Speed** of the interface.

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

7. **Step 7** (Optional) Choose the **Duplex** of the interface.
Step 8 Click OK.

Add an EtherChannel (Port Channel)

An EtherChannel (also known as a port channel) can include up to 16 member interfaces of the same type.

Note

When the chassis creates an EtherChannel, the EtherChannel stays in a Suspended state for Active LACP mode or a Down state for On LACP mode until you assign it to a logical device, even if the physical link is up.

Procedure

Step 1 Click Interfaces.

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

Step 2 Click Add New > Port Channel.

Step 3 Enter a Port Channel ID, between 1 and 47.

Step 4 Check the Enable check box.

Step 5 Choose the interface Type: Data, Data-sharing, Mgmt, or Firepower-eventing.
Do not choose the Cluster type.

Note There are limitations when using Data-sharing type interfaces; see the FXOS configuration guide for more information.

For Firepower-eventing, see the FMC configuration guide.

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

**Step 7** For Data or Data-sharing interfaces, choose the LACP port-channel Mode: Active or On.

For non-Data or non-Data-sharing interfaces, the mode is always active. You should use the active mode unless you need to minimize the amount of LACP traffic.

**Step 8** Set the **Admin Duplex** from the drop-down list.

**Step 9** To add an interface to the port channel, select the interface in the Available Interface list and click Add Interface to move it to the Member ID list.

You can add up to 16 interfaces of the same type and speed.

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

**Step 10** To remove an interface from the port channel, click the delete icon ( masse) to the right of the interface in the Member ID list.

**Step 11** Click OK.

---

**Add a VLAN Subinterface for Container Instances**

You can add up to 500 subinterfaces to your chassis. Subinterfaces are supported for container instances only; for more information, see Logical Device Application Instances: Container or Native, on page 3.

VLAN IDs per interface must be unique, and within a container instance, VLAN IDs must be unique across all assigned interfaces. You can reuse VLAN IDs on separate interfaces as long as they are assigned to different container instances. However, each subinterface still counts towards the limit even though it uses the same ID.

For native instances, you can create VLAN subinterfaces within the application only. For container instances, you can also create VLAN subinterfaces inside the application on interfaces that do not have FXOS VLAN subinterfaces defined, and these subinterfaces are not subject to the FXOS limit. Choosing in which operating system to create subinterfaces depends on your network deployment and personal preference. For example, to share a subinterface, you must create the subinterface in FXOS. Another scenario that favors FXOS subinterfaces comprises allocating separate subinterface groups on a single interface to multiple instances. For example, you want to use Port-channel1 with VLAN 2–11 on instance A, VLAN 12–21 on instance B, and VLAN 22–31 on instance C. If you create these subinterfaces within the application, then you would have to share the parent interface in FXOS, which may not be desirable. See the following illustration that shows the three ways you can accomplish similar scenarios:
Procedure

**Step 1**  
Click **Interfaces**.

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

**Step 2**  
Click **Add New > Subinterface** to open the **Add Subinterface** dialog box.

**Step 3**  
Choose the interface Type: **Data** or **Data-sharing**.
Subinterfaces are supported on Data or Data-sharing type interfaces only. The type is independent of the parent interface type; you can have a Data-sharing parent and a Data subinterface, for example.

**Note** There are limitations when using Data-sharing type interfaces; see the FXOS configuration guide for more information.

**Step 4** Choose the parent **Interface** from the drop-down list.

You cannot add a subinterface to a physical interface that is currently allocated to a logical device. If other subinterfaces of the parent are allocated, you can add a new subinterface as long as the parent interface itself is not allocated.

**Step 5** Enter a **Subinterface ID**, between 1 and 4294967295.

This ID will be appended to the parent interface ID as `interface_id.subinterface_id`. For example, if you add a subinterface to Ethernet1/1 with the ID of 100, then the subinterface ID will be: Ethernet1/1.100. This ID is not the same as the VLAN ID, although you can set them to match for convenience.

**Step 6** Set the **VLAN ID** between 1 and 4095.

**Step 7** Click **OK**.

Expand the parent interface to view all subinterfaces under it.

---

**Upload Software Images to the Chassis**

This procedure describes how to upload new FXOS and application images, as well as how to upgrade the FXOS image. You might need to upload new images if the pre-installed images are not the versions you require.

**Before you begin**

- Check compatibility between FXOS, ASA, and FTD versions in the FXOS compatibility guide.

- Make sure the image you want to upload is available on your local computer. To obtain FXOS and application software for the Firepower 4100, see:
  

- To make sure your upload succeeds during your HTTPS session, you might need to change the absolute timeout at the FXOS CLI. The absolute timeout is 60 minutes (the maximum), and large uploads might take longer than 60 minutes. To disable the absolute timeout, enter:
Procedure

Step 1  Check your current FXOS version by looking at the Overview page.

Step 2  Choose System > Updates.

Step 3  Click Upload Image to open the Upload Image dialog box.

Step 4  Click Browse to navigate to and select the image that you want to upload.

Step 5  Click Upload. The selected image is uploaded to the chassis.

Step 6  To upgrade the FXOS image:

   a)  Click the Upgrade icon ( ) for the FXOS platform bundle to which you want to upgrade.

   b)  Click Yes to confirm that you want to proceed with installation.

The chassis reloads. The upgrade process typically takes between 20 and 30 minutes.
## History for FXOS

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Version</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| VLAN subinterfaces for use with container instances       | 2.4.1   | To provide flexible physical interface use, you can create VLAN subinterfaces in FXOS and also share interfaces between multiple instances.  
  **Note** Requires FTD Version 6.3 or later.  
  New/Modified screens:  
  **Interfaces > All Interfaces > Add New** drop-down menu > **Subinterface**  
  New/Modified Firepower Management Center screens:  
  **Devices > Device Management > Edit** icon > **Interfaces**                                                                                         |
| Data-sharing interfaces for container instances            | 2.4.1   | To provide flexible physical interface use, you can share interfaces between multiple instances.  
  **Note** Requires FTD Version 6.3 or later.  
  New/Modified screens:  
  **Interfaces > All Interfaces > Type**                                                                                                               |
| Support for data EtherChannels in On mode                  | 2.4.1   | You can now set data and data-sharing EtherChannels to either Active LACP mode or to On mode. Other types of EtherChannels only support Active mode.  
  New/Modified screens:  
  **Interfaces > All Interfaces > Edit Port Channel > Mode**                                                                                          |
| Support for EtherChannels in FTD inline sets               | 2.1.1   | You can now use EtherChannels in a FTD inline set.                                                                                                                                                                     |
| Inline set link state propagation support for the FTD      | 2.0.1   | When you configure an inline set in the FTD application and enable link state propagation, the FTD sends inline set membership to the FXOS chassis. Link state propagation means that the chassis automatically brings down the second interface in the inline interface pair when one of the interfaces in an inline set goes down.  
  New/Modified commands: **show fault** |grep| **link-down**, **show interface detail**                                                                                                                  |
| Support for Hardware bypass network modules for the FTD    | 2.0.1   | Hardware Bypass ensures that traffic continues to flow between an inline interface pair during a power outage. This feature can be used to maintain network connectivity in the case of software or hardware failures.  
  New/Modified Firepower Management Center screens:  
  **Devices > Device Management > Interfaces > Edit Physical Interface**                                                                                   |
<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Version</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firepower-eventing type interface for FTD</td>
<td>1.1.4</td>
<td>You can specify an interface as firepower-eventing for use with the FTD. This interface is a secondary management interface for FTD devices. To use this interface, you must configure its IP address and other parameters at the FTD CLI. For example, you can separate management traffic from events (such as web events). See the &quot;Management Interfaces&quot; section in the Firepower Management Center configuration guide System Configuration chapter. New/Modified Firepower Chassis Manager screens: Interfaces &gt; All Interfaces &gt; Type</td>
</tr>
</tbody>
</table>
CHAPTER 2

Firepower Threat Defense Deployment with FDM

Is This Chapter for You?

This chapter describes how to deploy a standalone FTD logical device with Firepower Device Manager (FDM). To deploy a High Availability pair, see the FDM configuration guide.

FDM lets you configure the basic features of the software that are most commonly used for small networks. It is especially designed for networks that include a single device or just a few, where you do not want to use a high-powered multiple-device manager to control a large network containing many FDM devices.

If you are managing large numbers of devices, or if you want to use the more complex features and configurations that FTD allows, use the Firepower Management Center (FMC) instead.

Privacy Collection Statement—The Firepower 4100 does not require or actively collect personally-identifiable information. However, you can use personally-identifiable information in the configuration, for example for usernames. In this case, an administrator might be able to see this information when working with the configuration or when using SNMP.

• About Firepower Threat Defense with FDM, on page 23
• End-to-End Procedure, on page 24
• Firepower Chassis Manager: Add a Firepower Threat Defense Logical Device, on page 25
• Log Into FDM, on page 29
• Configure Licensing, on page 29
• Configure a Basic Security Policy, on page 35
• Access the Firepower Threat Defense CLI, on page 47
• What’s Next?, on page 49
• History for FTD with FDM, on page 50

About Firepower Threat Defense with FDM

The FTD provides next-generation firewall services, including stateful firewalling, routing, VPN, Next-Generation Intrusion Prevention System (NGIPS), Application Visibility and Control (AVC), URL filtering, and Advanced Malware Protection (AMP).

You can manage the FTD using the Firepower Device Manager (FDM), a simplified, single device manager included on the device. Use HTTPS to the Management interface that you allocated to the FTD logical device.
For troubleshooting purposes, you can access the FTD CLI using SSH on the Management interface, or you can connect to the FTD from the FXOS CLI.

## End-to-End Procedure

See the following tasks to deploy and configure the FTD on your chassis.

<table>
<thead>
<tr>
<th>Workspace</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firepower Chassis Manager</td>
<td>Firepower Chassis Manager: Add a Firepower Threat Defense Logical Device, on page 25.</td>
</tr>
<tr>
<td>FDM</td>
<td>Log Into FDM, on page 29.</td>
</tr>
<tr>
<td>Cisco Commerce Workspace</td>
<td>Configure Licensing, on page 29: Buy feature licenses.</td>
</tr>
<tr>
<td>Smart Software Manager</td>
<td>Configure Licensing, on page 29: Generate a license token for the FTD.</td>
</tr>
</tbody>
</table>
Firepower Chassis Manager: Add a Firepower Threat Defense Logical Device

You can deploy an FTD from the Firepower 4100 as a native instance. Container instances are not supported. To add a High Availability pair, see the FDM configuration guide.

Before you begin

- Configure a Management interface to use with the FTD; see Configure Interfaces, on page 14. The Management interface is required. Note that this Management interface is not the same as the chassis management port that is used only for chassis management (and that appears at the top of the Interfaces tab as MGMT).
- You must also configure at least one Data interface.
- Gather the following information:
  - Interface IDs for this device
  - Management interface IP address and network mask
  - Gateway IP address
  - DNS server IP address
  - FTD hostname and domain name

Procedure

Step 1
In Firepower Chassis Manager, choose Logical Devices.

Step 2
Click Add > Standalone, and set the following parameters:

![Add Standalone](image)

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

b) For the Template, choose Cisco Firepower Threat Defense.

c) Choose the Image Version.

d) Choose the Instance Type: Native.

Container instances are not supported with FDM.

e) Click OK.

You see the Provisioning - device name window.

**Step 3**

Expand the Data Ports area, and click each interface that you want to assign to the device.

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

**Step 4**

Click the device icon in the center of the screen.

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

**Step 5**

On the General Information page, complete the following:
a) Choose the Management Interface.
   This interface is used to manage the logical device. This interface is separate from the chassis management port.

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

c) Configure the Management IP address.
   Set a unique IP address for this interface.

d) Enter a Network Mask or Prefix Length.

e) Enter a Network Gateway address.

Step 6  On the Settings tab, complete the following:
a) In the **Management type of application instance** drop-down list, choose **LOCALLY_MANAGED**. Native instances also support FMC as a manager. If you change the manager after you deploy the logical device, then your configuration is erased and the device is reinitialized.

b) Enter the **Search Domains** as a comma-separated list.

c) The **Firewall Mode** only supports **Routed** mode.

d) Enter the **DNS Servers** as a comma-separated list.

e) Enter the **Fully Qualified Hostname** for the FTD.

f) Enter a **Password** for the FTD admin user for CLI access.

**Step 7**  
On the **Agreement** tab, read and accept the end user license agreement (EULA).

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

**Step 9**  
Click **Save**.

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

Log into FDM to configure your FTD.

Before you begin

• Use a current version of Firefox, Chrome, Safari, Edge, or Internet Explorer.

• Make sure the ASA logical device Status is online on the Firepower Chassis Manager Logical Devices page.

Procedure

Step 1
Enter the following URL in your browser.

• `https://management_ip`—Management interface IP address that you entered in the bootstrap configuration.

Step 2
Log in with the username admin, and the password you set when you deployed the FTD.

Step 3
You are prompted to accept the 90-day evaluation license.

Configure Licensing

The FTD uses Cisco Smart Software Licensing, which lets you purchase and manage a pool of licenses centrally.

When you register the chassis, the License Authority issues an ID certificate for communication between the chassis and the License Authority. It also assigns the chassis to the appropriate virtual account.

The Base license is included automatically. Smart Licensing does not prevent you from using product features that you have not yet purchased, but you should purchase the following optional feature licenses to be in compliance:
Configure Licensing

- **Threat**—Security Intelligence and Cisco Firepower Next-Generation IPS
- **Malware**—Advanced Malware Protection for Networks (AMP)
- **URL**—URL Filtering
- **RA VPN**—AnyConnect Plus, AnyConnect Apex, or AnyConnect VPN Only.

In addition to the above licenses, you also need to buy a matching subscription to access updates for 1, 3, or 5 years.

For complete information on licensing your system, see the [FDM configuration guide](#).

**Before you begin**

- Have a master account on the Cisco Smart Software Manager.

  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.

- Your Cisco Smart Software Licensing account must qualify for the Strong Encryption (3DES/AES) license to use some features (enabled using the export-compliance flag).

**Procedure**

**Step 1**

Make sure your Smart Licensing account contains the available licenses you need.

When you bought your device from Cisco or a reseller, your licenses should have been linked to your Smart Software License account. However, if you need to add licenses yourself, use the **Find Products and Solutions** search field on the Cisco Commerce Workspace. Search for the following license PIDs:

*Figure 1: License Search*

- **Note** If a PID is not found, you can add the PID manually to your order.

  - Threat, Malware, and URL license combination:
    - L-FPR4110T-TMC=
    - L-FPR4120T-TMC=
    - L-FPR4140T-TMC=
    - L-FPR4150T-TMC=

  - Threat, Malware, and URL subscription combination:
    - L-FPR4110T-TMC-1Y
• L-FPR4110T-TMC-3Y
• L-FPR4110T-TMC-5Y
• L-FPR4120T-TMC-1Y
• L-FPR4120T-TMC-3Y
• L-FPR4120T-TMC-5Y
• L-FPR4140T-TMC-1Y
• L-FPR4140T-TMC-3Y
• L-FPR4140T-TMC-5Y
• L-FPR4150T-TMC-1Y
• L-FPR4150T-TMC-3Y
• L-FPR4150T-TMC-5Y

• RA VPN—See the Cisco AnyConnect Ordering Guide.

**Step 2**  
In the Cisco Smart Software Manager, request and copy a registration token for the virtual account to which you want to add this device.  
a) Click **Inventory**.  

![Cisco Software Central > Smart Software Licensing](image)  

Smart Software Licensing  

<table>
<thead>
<tr>
<th>Alerts</th>
<th>Inventory</th>
<th>License Conversion</th>
<th>Reports</th>
<th>Email Notification</th>
<th>Satellites</th>
<th>Activity</th>
</tr>
</thead>
</table>

b) On the **General** tab, click **New Token**.  

c) On the **Create Registration Token** dialog box enter the following settings, and then click **Create Token**:
• Description

• **Expire After**—Cisco recommends 30 days.

• **Allow export-controlled functionality on the products registered with this token**—Enables the export-compliance flag if you are in a country that allows for strong encryption.

The token is added to your inventory.

d) Click the arrow icon to the right of the token to open the **Token** dialog box so you can copy the token ID to your clipboard. Keep this token ready for later in the procedure when you need to register the FTD.

**Figure 2: View Token**

<table>
<thead>
<tr>
<th>General</th>
<th>Licenses</th>
<th>Product Instances</th>
<th>Event Log</th>
</tr>
</thead>
</table>

**Virtual Account**

- Description: [Your Description]
- Default Virtual Account: [Yes/No]

**Product Instance Registration Tokens**
The registration tokens below can be used to register new product instances to this virtual account.

**Figure 3: Copy Token**

**Step 3** In FDM, click **Device**, and then in the **Smart License** summary, click **View Configuration**.

You see the **Smart License** page.

**Step 4** Click **Register Device**.
Then follow the instructions on the **Smart License Registration** dialog box to paste in your token:

1. **Create or log in into your Cisco Smart Software Manager account.**
2. **On your assigned virtual account, under “General tab”, click on “New Token” to create token.**
3. **Copy the token and paste it here:**
   ```text
   MGY2NzMywGh0DJ/2/00NzF1LWJiNiZYWmNzLIO0Y22YVlLTe1NiUz
   Zh%Q66eG5Mz8YSUGVm58ozZISmS5N36K3ow23ovVmpmc3Yta1
   J6O2Fr6G8eWw%AWC9WT%0%DA
   ```
4. **Select Region**
   When you register the device, you are also registered with Cisco Security Services Exchange (SSE). Please select the region in which your device is operating. You will be able to see your device in the device list of the regional SSE portal.
   ```text
   Region:
   SSE US Region
   ```
5. **Cisco Success Network**
   Cisco Success Network enables provide usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.
   ```text
   Check out the Sample Data that will be sent to Cisco. See more
   ```
   ```text
   ✔ Enable Cisco Success Network
   ```

---

**Step 5**

Click **Register Device**.

You return to the **Smart License** page. While the device registers, you see the following message:

Registration request sent on 10 Jul 2019. Please wait. Normally, it takes about one minute to complete the registration. You can check the task status in Task List. Refresh this page to see the updated status.

After the device successfully registers and you refresh the page, you see the following:
Step 6  Click the Enable/Disable control for each optional license as desired.

- **Enable**—Registers the license with your Cisco Smart Software Manager account and enables the controlled features. You can now configure and deploy policies controlled by the license.

- **Disable**—Unregisters the license with your Cisco Smart Software Manager account and disables the controlled features. You cannot configure the features in new policies, nor can you deploy policies that use the feature.

- If you enabled the RA VPN license, select the type of license you want to use: **Plus**, **Apex**, **VPN Only**, or **Plus and Apex**.

After you enable features, if you do not have the licenses in your account, you will see the following non-compliance message after you refresh the page:
Step 7  Choose Resync Connection from the gear drop-down list to synchronize license information with Cisco Smart Software Manager.

Configure a Basic Security Policy

To configure a basic security policy, complete the following tasks.

1. Configure Interfaces, on page 35.
   Assign a static IP address to the inside interface, and use DHCP for the outside interface.

2. Add Interfaces to Security Zones, on page 38.
   Add the inside and outside interfaces to inside and outside security zones, which are required for access control.

3. Add the Default Route, on page 39.
   If you do not receive the default route from the outside DHCP server, you need to manually add it.

4. Configure NAT, on page 41.
   Use interface PAT on the outside interface.

5. Allow Traffic from Inside to Outside, on page 43.
   Allow traffic from inside to outside.

6. (Optional) Configure the DHCP Server, on page 44.
   Use a DHCP server on the inside interface for clients.

7. (Optional) Configure the Management Gateway and Allow Management on Data Interfaces, on page 45.
   Change the management gateway and/or allow management from a data interface.

8. Deploy the Configuration, on page 47.

Configure Interfaces

Enable FTD interfaces and set the IP addresses. Typically, you must configure at least a minimum of two interfaces to have a system that passes meaningful traffic. Normally, you would have an outside interface that faces the upstream router or internet, and one or more inside interfaces for your organization’s networks.
Some of these interfaces might be “demilitarized zones” (DMZs), where you place publically-accessible assets such as your web server.

A typical edge-routing situation is to obtain the outside interface address through DHCP from your ISP, while you define static addresses on the inside interfaces.

The following example configures an inside interface with a static address and an outside interface using DHCP.

**Procedure**

**Step 1** Click Device, and then click the link in the Interfaces summary.

The Interfaces page is selected by default. The interfaces list shows physical interfaces, their names, addresses, and states.

**Step 2** Click the edit icon (📝) for the interface that you want to use for inside.

**Step 3** Set the following:

![Ethernet1/2 Edit Physical Interface](image)

- **Interface Name**: Set the Interface Name.
- **Mode**: Static
- **IP Address and Subnet Mask**:
  - 10.99.10.1 / 24
  - e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0
- **Standby IP Address and Subnet Mask**:
  - 10.99.10.2 / 24
  - e.g. 192.168.5.16

a) Set the Interface Name.
Set the name for the interface, up to 48 characters. Alphabetic characters must be lower case. For example, `inside` or `outside`. Without a name, the rest of the interface configuration is ignored. Unless you configure subinterfaces, the interface should have a name.

b) Set the **Mode** to **Routed**.

   If you want to use Passive interfaces, see the [FDM configuration guide](#).

c) Set the **Status** slider to the enabled setting ( ).

   **Important** You must also enable the interface in FXOS.

d) (Optional) Set the **Description**.

   The description can be up to 200 characters on a single line, without carriage returns.

e) On the **IPv4 Address** page, configure a static IP address.

f) (Optional) Click **IPv6 Address**, and configure IPv6.

**Step 4**

Click **OK**.

**Step 5**

Click the edit icon ( ) for the interface that you want to use for `outside`, and set the same fields as for inside; for this interface, choose **DHCP** for the IPv4 Address.

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>Mode</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>outside</td>
<td>Routed</td>
<td></td>
</tr>
</tbody>
</table>

*Important* If the DHCP server supplies an address on the same network configured statically for another interface, this interface will be disabled. Ensure that there is no overlap between the network addresses on this interface and the other interfaces on the device.
If you use a static IP address or do not receive the default route from DHCP, you will need to manually set a default route; see the FDM configuration guide.

### Add Interfaces to Security Zones

A security zone is a grouping of interfaces. Zones divide the network into segments to help you manage and classify traffic. You can define multiple zones, but a given interface can be in one zone only.

This procedure tells you how to add interfaces to the following pre-configured zones:

- **inside_zone**—This zone is intended to represent internal networks.
- **outside_zone**—This zone is intended to represent networks external to your control, such as the Internet.

### Procedure

1. Select **Objects**, then select **Security Zones** from the table of contents.
2. Click the edit icon (![](https://www.cisco.com/c/en/us/td/docs/security/firepower/ftdd/fdm/5.0/gs/quickrefemanuallysetdefaultroute.html)) for the **inside_zone**.
3. In the **Interfaces** list, click + and select the inside interface to add to the zone.
4. Click OK to save your changes.
Step 5
Repeat these steps to add the outside interface to the outside Zone.

Edit Security Zone

Add the Default Route

The default route normally points to the upstream router reachable from the outside interface. If you use DHCP for the outside interface, your device might have already received a default route. If you need to manually add the route, complete this procedure. If you received a default route from the DHCP server, it will show on the Device Summary > Static Routing page.

Procedure

Step 1
Click Device, then click the link in the Routing summary.

The Static Routing page appears.

Step 2
Click + or Create Static Route.

Step 3
Configure the default route properties.
Add the Default Route

a) Enter a Name, for example, default.

b) Click either the IPv4 or IPv6 radio button.

   You need to create separate default routes for IPv4 and IPv6.

c) Click Gateway, and then click Create New Network to add the gateway IP address as a host object.
d) Choose the gateway **Interface**, for example **outside**.

e) Click the **Networks** icon, and choose **any-ipv4** for an IPv4 default route or **any-ipv6** for an IPv6 default route.

**Step 4** Click **OK**.

---

**Configure NAT**

A typical NAT rule converts internal addresses to a port on the outside interface IP address. This type of NAT rule is called **interface Port Address Translation (PAT)**. You cannot use interface PAT for IPv6.

**Procedure**

**Step 1** Click **Policies** and then click **NAT**.

**Step 2** Click **+** or Create NAT Rule.

**Step 3** Configure the basic rule options:
a) Set the **Title**.

b) Choose **Create Rule For > Auto NAT**.

c) Choose **Type > Dynamic**.

**Step 4**  Configure the following packet translation options:

a) For the **Original Packet**, set the **Original Address** as **any-ipv4**.

   This rule will translate all IPv4 traffic originating on any interface. If you want to restrict the interfaces or the addresses, you can choose a specific **Source Interface** and specify IP addresses for the **Original Address**.

b) For the **Translated Packet**, set the **Destination Interface** to the outside interface.

   By default, the interface IP address is used for the translated address.

**Step 5**  (Optional) Click **Show Diagram** to view a visual representation of the rule.
Step 6  Click OK.

Allow Traffic from Inside to Outside

By default, traffic is blocked between security zones. This procedure shows how to allow traffic from inside to outside.

Procedure

Step 1  Choose Policies > Access Control.
Step 2  Click † or Create Access Rule.
Step 3  Configure the basic rule options:

- a) Set the Title.
- b) For the Source, click the Zones † icon, and choose the inside zone.
c) For the **Destination**, click the **Zones** icon, and choose the outside zone.

d) (Optional) Click **Show Diagram** to view a visual representation of the rule.

e) Click **OK**.

---

### (Optional) Configure the DHCP Server

Enable the DHCP server if you want clients to use DHCP to obtain IP addresses from the FTD.

**Procedure**

**Step 1**  
Click **Device**, then click the **System Settings > DHCP Server** link.

**Step 2**  
Click **+** or **Create DHCP Server**.

**Step 3**  
Configure the server properties.

![Add Server](image)

- **Enabled DHCP Server**: On
- **Interface**: Inside
- **Address Pool**: 10.99.10.5-10.99.10.254

**Step 4**  
(Optional) Click **Configuration** to configure auto-configuration and global settings.
DHCP auto configuration enables the DHCP Server to provide DHCP clients with DNS server, domain name, and WINS server information obtained from a DHCP client that is running on the specified interface. Typically, you would use auto-configuration if you are obtaining an address using DHCP on the outside interface, but you could choose any interface that obtains its address through DHCP. If you cannot use auto-configuration, you can manually define the required options.

a) Click the Enable Auto Configuration slider so that it shows enabled ( ).

b) Choose the interface in the From Interface drop-down menu from which you want clients to inherit server settings.

c) If you do not enable auto-configuration, or if you want to override any of the automatically configured settings, configure one or more global options. These settings will be sent to DHCP clients on all interfaces that run a DHCP server.

d) Click Save.

(Optional) Configure the Management Gateway and Allow Management on Data Interfaces

When you deployed the FTD, you configured the management address and an external gateway. The following procedure lets you configure the FTD to send management traffic over the backplane through the data interfaces instead of through the management interface. In this case, you can still manage the FTD if you are on a
directly-connected management network, but management traffic destined for any other network will be routed out the data interfaces instead of through management.

Also, by default, you can only manage the FTD through the management interface (FDM or CLI access). The following procedure also lets you enable management on one or more data interfaces. Note that the management interface gateway does not affect FDM management traffic on data interfaces; in this case, the FTD uses the regular routing table.

**Before you begin**

Configure data interfaces according to Configure Interfaces, on page 35.

**Procedure**

**Step 1** Allow management from a data interface.

a) Click Device, then click the System Settings > Management Access link.
b) Click Data Interfaces.
c) Click + or Create Data Interface, and create a rule for each interface:

![Add Management Access](image)

- **Interface**—Choose the interface on which you want to allow management access.
- **Protocols**—Choose whether the rule is for HTTPS (port 443), SSH (port 22), or both.
- **Allowed Networks**—Choose the network objects that define the IPv4 or IPv6 network or host that should be able to access the system. To specify "any" address, select any-ipv4 (0.0.0.0/0) and any-ipv6 (::/0).

d) Click OK.

**Step 2** Set the management gateway to use the data interfaces.

a) Click Device, then click the System Settings > Management Interface link.
b) Choose Use the Data Interfaces as the Gateway.
c) Click Save, read the warning, and click OK.

### Deploy the Configuration

Deploy the configuration changes to the FTD; none of your changes are active on the device until you deploy them.

**Procedure**

**Step 1**
Click the **Deploy Changes** icon in the upper right of the web page.

The icon is highlighted with a dot when there are undeployed changes.

The Pending Changes window shows a comparison of the deployed version of the configuration with the pending changes. These changes are color-coded to indicate removed, added, or edited elements. See the legend in the window for an explanation of the colors.

**Step 2**
If you are satisfied with the changes, you can click **Deploy Now** to start the job immediately.

The window will show that the deployment is in progress. You can close the window, or wait for deployment to complete. If you close the window while deployment is in progress, the job does not stop. You can see results in the task list or audit log. If you leave the window open, click the **Deployment History** link to view the results.

### Access the Firepower Threat Defense CLI

You can use the FTD CLI to change management interface parameters and for troubleshooting purposes. You can access the CLI using SSH to the Management interface, or by connecting from the FXOS CLI.
Procedure

Step 1 (Option 1) SSH directly to the FTD management interface IP address.
You set the management IP address when you deployed the logical device. Log into the FTD with the admin
account and the password you set during initial deployment.
If you forgot the password, you can change it by editing the logical device in the Firepower Chassis Manager.

Step 2 (Option 2) From the FXOS CLI, connect to the module CLI using a console connection or a Telnet connection.

a) Connect to the security engine.

```
connect module 1 {console | telnet}
```

The benefits of using a Telnet connection is that you can have multiple sessions to the module at the same
time, and the connection speed is faster.

```
Example:

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

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

b) Connect to the FTD console.

```
connect ftd name
```
If you have multiple application instances, you must specify the name of the instance. To view the instance
names, enter the command without a name.

```
Example:

Firepower-module1> connect ftd FTD_Instance1

---------------------------- ATTENTION ----------------------------
You are connecting to ftd from a serial console. Please avoid
executing any commands which may produce large amount of output.
Otherwise, data cached along the pipe may take up to 12 minutes to be
drained by a serial console at 9600 baud rate after pressing Ctrl-C.

To avoid the serial console, please login to FXOS with ssh and use
'connect module <slot> telnet' to connect to the security module.

Connecting to container ftd(FTD_Instance1) console... enter "exit" to return to bootCLI
```

c) Exit the application console to the FXOS module CLI by entering exit.

Note For pre-6.3 versions, enter Ctrl-a, d.
d) Return to the supervisor level of the FXOS CLI.

To exit the console:

1. Enter ~
   
   You exit to the Telnet application.

2. To exit the Telnet application, enter:
   
   telnet> quit

To exit the Telnet session:

Enter Ctrl-], .

---

Example

The following example connects to an FTD and then exits back to the supervisor level of the FXOS CLI.

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

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1> connect ftd FTD_Instance1

---------------------------------------- ATTENTION ----------------------------------------
You are connecting to ftd from a serial console. Please avoid executing any commands which may produce large amount of output. Otherwise, data cached along the pipe may take up to 12 minutes to be drained by a serial console at 9600 baud rate after pressing Ctrl-C.

To avoid the serial console, please login to FXOS with ssh and use "connect module <slot> telnet" to connect to the security module.

----------------------------------------

Connecting to container ftd(FTD_Instance1) console... enter "exit" to return to bootCLI
> ~
telnet> quit
Connection closed.
Firepower#
```

What's Next?

To continue configuring your FTD device, see the documents available for your software version at Navigating the Cisco Firepower Documentation.
For information related to using FDM, see Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager.

## History for FTD with FDM

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Version</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for FDM with native instances</td>
<td>6.5.0</td>
<td>You can now deploy a native instance using FDM.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>New/Modified screens:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Logical Devices</strong> &gt; <strong>Add Device</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Is This Chapter for You?

This chapter describes how to deploy a standalone FTD logical device with FMC. To deploy a High Availability pair or a cluster, see the FMC configuration guide.

In a typical deployment on a large network, multiple managed devices are installed on network segments, monitor traffic for analysis, and report to a managing FMC, which provides a centralized management console with web interface that you can use to perform administrative, management, analysis, and reporting tasks.

For networks that include only a single device or just a few, where you do not need to use a high-powered multiple-device manager like the FMC, you can use the integrated Firepower Device Manager (FDM). Use the FDM web-based device setup wizard to configure the basic features of the software that are most commonly used for small network deployments.

Privacy Collection Statement—The Firepower 4100 does not require or actively collect personally-identifiable information. However, you can use personally-identifiable information in the configuration, for example for usernames. In this case, an administrator might be able to see this information when working with the configuration or when using SNMP.
About Firepower Threat Defense with FMC

The FTD provides next-generation firewall services, including stateful firewalling, routing, VPN, Next-Generation Intrusion Prevention System (NGIPS), Application Visibility and Control (AVC), URL filtering, and Advanced Malware Protection (AMP).

You can manage the FTD using the Firepower Management Center (FMC), a full-featured, multidevice manager on a separate server.

The FTD registers and communicates with the FMC on the Management interface that you allocated to the FTD logical device.

For troubleshooting purposes, you can access the FTD CLI using SSH on the Management interface, or you can connect to the FTD from the FXOS CLI.

Before You Start

Deploy and perform initial configuration of the FMC. See the FMC getting started guide.

Note

The Firepower device and the FMC both have the same default management IP address: 192.168.45.45. This guide assumes that you will set different IP addresses for your devices during initial setup.

End-to-End Procedure

See the following tasks to deploy and configure the FTD on your chassis.
### Firepower Threat Defense Deployment with FMC

#### End-to-End Procedure

<table>
<thead>
<tr>
<th>Workspace</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong> Firepower Chassis Manager</td>
<td>Firepower Chassis Manager: Add a Firepower Threat Defense Logical Device, on page 54.</td>
</tr>
<tr>
<td><strong>2</strong> FMC</td>
<td>Log Into the Firepower Management Center, on page 58.</td>
</tr>
<tr>
<td><strong>3</strong> Cisco Commerce Workspace</td>
<td>Obtain Licenses for the Firepower Management Center, on page 59: Buy feature licenses.</td>
</tr>
<tr>
<td><strong>4</strong> Smart Software Manager</td>
<td>Obtain Licenses for the Firepower Management Center, on page 59: Generate a license token for the FMC.</td>
</tr>
<tr>
<td><strong>5</strong> FMC</td>
<td>Obtain Licenses for the Firepower Management Center, on page 59: Register the FMC with the Smart Licensing server.</td>
</tr>
<tr>
<td><strong>6</strong> FMC</td>
<td>Register the Firepower Threat Defense with the Firepower Management Center, on page 61.</td>
</tr>
<tr>
<td><strong>7</strong> FMC</td>
<td>Configure a Basic Security Policy, on page 63.</td>
</tr>
</tbody>
</table>
Firepower Chassis Manager: Add a Firepower Threat Defense Logical Device

You can deploy an FTD from the Firepower 4100 as either a native or container instance. You can deploy multiple container instances per security engine, but only one native instance. See Logical Device Application Instances: Container or Native, on page 3 for the maximum container instances per model.

To add a High Availability pair or a cluster, see the FMC configuration guide.

This procedure lets you configure the logical device characteristics, including the bootstrap configuration used by the application.

Before you begin

• Configure a Management interface to use with the FTD; see Configure Interfaces, on page 14. The Management interface is required. Note that this Management interface is not the same as the chassis management port that is used only for chassis management (and that appears at the top of the Interfaces tab as MGMT).

• You must also configure at least one Data interface.

• For container instances, if you do not want to use the default profile, which uses the minimum resources, add a resource profile on Platform Settings > Resource Profiles.

• For container instances, before you can install a container instance for the first time, you may need to reinitialize the security engine so that the disk has the correct formatting. If this action is required, you will not be able to save your logical device. Click Security Engine, and then click the Reinitialize icon (§).

• Gather the following information:
  • Interface IDs for this device
  • Management interface IP address and network mask
  • Gateway IP address
  • FMC IP address and/or NAT ID of your choosing
  • DNS server IP address

Procedure

Step 1 In Firepower Chassis Manager, choose Logical Devices.

Step 2 Click Add > Standalone, and set the following parameters:
a) Provide a **Device Name**.
   This name is used by the chassis supervisor to configure management settings and to assign interfaces; it is not the device name used in the application configuration.

b) For the **Template**, choose **Cisco Firepower Threat Defense**.

c) Choose the **Image Version**.

d) Choose the **Instance Type**: **Container** or **Native**.
   A native instance uses all of the resources (CPU, RAM, and disk space) of the security module/engine, so you can only install one native instance. A container instance uses a subset of resources of the security module/engine, so you can install multiple container instances.

e) Click **OK**.
   You see the Provisioning - **device name** window.

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

You can only assign Data and Data-sharing interfaces that you previously enabled on the **Interfaces** page. You will later enable and configure these interfaces in FMC, including setting the IP addresses.
You can only assign up to 10 Data-sharing interfaces to a container instance. Also, each Data-sharing interface can be assigned to at most 14 container instances. A Data-sharing interface is indicated by the sharing icon ( ).

Hardware Bypass–capable ports are shown with the following icon: . For certain interface modules, you can enable the Hardware Bypass feature for Inline Set interfaces only (see the FMC configuration guide for information about Inline Sets). Hardware Bypass ensures that traffic continues to flow between an inline interface pair during a power outage. This feature can be used to maintain network connectivity in the case of software or hardware failures. If you do not assign both interfaces in a Hardware Bypass pair, you see a warning message to make sure your assignment is intentional. You do not need to use the Hardware Bypass feature, so you can assign single interfaces if you prefer.

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

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

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

<table>
<thead>
<tr>
<th>Cisco Firepower Threat Defense - Bootstrap Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Information</strong></td>
</tr>
<tr>
<td>SM 1 - 22 Cores Available</td>
</tr>
<tr>
<td>Interface Information</td>
</tr>
<tr>
<td>Management Interface: Ethernet 1/8</td>
</tr>
<tr>
<td>Management Address Type:</td>
</tr>
<tr>
<td>IPv4 Management IP:</td>
</tr>
<tr>
<td>Network Mask:</td>
</tr>
<tr>
<td>Network Gateway:</td>
</tr>
</tbody>
</table>

a) For a container instance, specify the **Resource Profile**.

If you later assign a different resource profile, then the instance will reload, which can take approximately 5 minutes. Note that for established High Availability pairs or clusters, if you assign a different-sized resource profile, be sure to make all members the same size as soon as possible.

b) Choose the **Management Interface**.

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

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

d) Configure the **Management IP** address.
Set a unique IP address for this interface.
e) Enter a **Network Mask** or **Prefix Length**.
f) Enter a **Network Gateway** address.

**Step 6** On the **Settings** tab, complete the following:

<table>
<thead>
<tr>
<th>Cisco Firepower Threat Defense - Bootstrap Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Information</strong></td>
</tr>
<tr>
<td>Management type of application instance:</td>
</tr>
<tr>
<td>Firepower Management Center IP:</td>
</tr>
<tr>
<td>Search domains:</td>
</tr>
<tr>
<td>Firewall Mode:</td>
</tr>
<tr>
<td>DNS Servers:</td>
</tr>
<tr>
<td>Firepower Management Center NAT ID:</td>
</tr>
<tr>
<td>Fully Qualified Hostnames:</td>
</tr>
<tr>
<td>Registration Key:</td>
</tr>
<tr>
<td>Confirm Registration Key:</td>
</tr>
<tr>
<td>Password:</td>
</tr>
<tr>
<td>Confirm Password:</td>
</tr>
<tr>
<td>Default Interface:</td>
</tr>
</tbody>
</table>

a) For a native instance, in the **Management type of application instance** drop-down list, choose **FMC**. Native instances also support FDM as a manager. After you deploy the logical device, you cannot change the manager type.

b) Enter the **Firepower Management Center IP** of the managing FMC. If you do not know the FMC IP address, leave this field blank and enter a passphrase in the **Firepower Management Center NAT ID** field.

c) For a container instance, **Permit Expert mode from FTD SSH sessions**: **Yes** or **No**. Expert Mode provides FTD shell access for advanced troubleshooting.

If you choose **Yes** for this option, then users who access the container instance directly from an SSH session can enter Expert Mode. If you choose **No**, then only users who access the container instance from the FXOS CLI can enter Expert Mode. We recommend choosing **No** to increase isolation between instances.

Use Expert Mode only if a documented procedure tells you it is required, or if the Cisco Technical Assistance Center asks you to use it. To enter this mode, use the **expert** command in the FTD CLI.

d) Enter the **Search Domains** as a comma-separated list.

e) Choose the **Firewall Mode**: **Transparent** or **Routed**.

In routed mode, the FTD is considered to be a router hop in the network. Each interface that you want to route between is on a different subnet. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a “bump in the wire,” or a “stealth firewall,” and is not seen as a router hop to connected devices.
The firewall mode is only set at initial deployment. If you re-apply the bootstrap settings, this setting is not used.

f) Enter the **DNS Servers** as a comma-separated list.

The FTD uses DNS if you specify a hostname for the FMC, for example.

g) Enter the **Fully Qualified Hostname** for the FTD.

h) Enter a **Registration Key** to be shared between the FMC and the device during registration.

You can choose any text string for this key between 1 and 37 characters; you will enter the same key on the FMC when you add the FTD.

i) Enter a **Password** for the FTD admin user for CLI access.

j) Choose the **Eventing Interface** on which Firepower events should be sent. If not specified, the management interface will be used.

This interface must be defined as a Firepower-eventing interface.

k) For a container instance, set the **Hardware Crypto** as **Enabled** or **Disabled**.

This setting enables TLS crypto acceleration in hardware, and improves performance for certain types of traffic. For more information, see the FMC configuration guide. This feature is not supported for native instances. To view the percentage of hardware crypto resources allocated to this instance, enter the `show hw-crypto` command.

**Step 7** On the **Agreement** tab, read and accept the end user license agreement (EULA).

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

**Step 9** Click **Save**.

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

---

**Log Into the Firepower Management Center**

Use the FMC to configure and monitor the FTD.
Before you begin

For information on supported browsers, refer to the release notes for the version you are using (see https://www.cisco.com/go/firepower-notes).

Procedure

Step 1
Using a supported browser, enter the following URL.

https://fmc_ip_address

Step 2
Enter your username and password.

Step 3
Click Log In.

Obtain Licenses for the Firepower Management Center

All licenses are supplied to the FTD by the FMC. You can optionally purchase the following feature licenses:

- **Threat**—Security Intelligence and Cisco Firepower Next-Generation IPS
- **Malware**—Advanced Malware Protection for Networks (AMP)
- **URL**—URL Filtering
- **RA VPN**—AnyConnect Plus, AnyConnect Apex, or AnyConnect VPN Only.

In addition to the above licenses, you also need to buy a matching subscription to access updates for 1, 3, or 5 years.

Before you begin

- Have a master account on the Cisco Smart Software Manager.
  
  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.

- Your Cisco Smart Software Licensing account must qualify for the Strong Encryption (3DES/AES) license to use some features (enabled using the export-compliance flag).

Procedure

Step 1
Make sure your Smart Licensing account contains the available licenses you need.

When you bought your device from Cisco or a reseller, your licenses should have been linked to your Smart Software License account. However, if you need to add licenses yourself, use the Find Products and Solutions search field on the Cisco Commerce Workspace. Search for the following license PID:
If a PID is not found, you can add the PID manually to your order.

- Threat, Malware, and URL license combination:
  - L-FPR4110T-TMC=
  - L-FPR4120T-TMC=
  - L-FPR4140T-TMC=
  - L-FPR4150T-TMC=

- Threat, Malware, and URL subscription combination:
  - L-FPR4110T-TMC-1Y
  - L-FPR4110T-TMC-3Y
  - L-FPR4110T-TMC-5Y
  - L-FPR4120T-TMC-1Y
  - L-FPR4120T-TMC-3Y
  - L-FPR4120T-TMC-5Y
  - L-FPR4140T-TMC-1Y
  - L-FPR4140T-TMC-3Y
  - L-FPR4140T-TMC-5Y
  - L-FPR4150T-TMC-1Y
  - L-FPR4150T-TMC-3Y
  - L-FPR4150T-TMC-5Y

- RA VPN—See the Cisco AnyConnect Ordering Guide.

**Step 2**

If you have not already done so, register the FMC with the Smart Licensing server.

Registering requires you to generate a registration token in the Smart Software Manager. See the FMC configuration guide for detailed instructions.
Register the Firepower Threat Defense with the Firepower Management Center

Register each logical device individually to the same FMC.

Before you begin

• Make sure the FTD logical device Status is online on the Firepower Chassis Manager Logical Devices page.

• Gather the following information that you set in the FTD initial bootstrap configuration (see Firepower Chassis Manager: Add a Firepower Threat Defense Logical Device, on page 54):
  • FTD management IP address and/or NAT ID
  • FMC registration key

Procedure

Step 1
In FMC, choose Devices > Device Management.

Step 2
From the Add drop-down list, choose Add Device, and enter the following parameters.

- **Host**: Enter the IP address of the FTD you want to add. You can leave this field blank if you specified both the FMC IP address and a NAT ID in the FTD initial bootstrap configuration.
• **Display Name**—Enter the name for the FTD as you want it to display in the FMC.

• **Registration Key**—Enter the same registration key that you specified in the FTD initial bootstrap configuration.

• **Domain**—Assign the device to a leaf domain if you have a multidomain environment.

• **Group**—Assign it to a device group if you are using groups.

• **Access Control Policy**—Choose an initial policy. Unless you already have a customized policy you know you need to use, choose Create new policy, and choose Block all traffic. You can change this later to allow traffic; see Allow Traffic from Inside to Outside, on page 71.

![New Policy](image)

• **Smart Licensing**—Assign the Smart Licenses you need for the features you want to deploy: Malware (if you intend to use AMP malware inspection), Threat (if you intend to use intrusion prevention), and URL (if you intend to implement category-based URL filtering).

• **Unique NAT ID**—Specify the NAT ID you specified in the FTD initial bootstrap configuration.

• **Transfer Packets**—Allow the device to transfer packets to the FMC. When events like IPS or Snort are triggered with this option enabled, the device sends event metadata information and packet data to the FMC for inspection. If you disable it, only event information will be sent to the FMC, but packet data is not sent.

**Step 3**  
Click Register, and confirm a successful registration.

If the registration succeeds, the device is added to the list. If it fails, you will see an error message. If the FTD fails to register, check the following items:

• **Ping**—Access the FTD CLI (Access the Firepower Threat Defense CLI, on page 73), and ping the FMC IP address using the following command:

```
ping system ip_address
```

If the ping is not successful, check your network settings using the `show network` command. If you need to change the FTD IP address, use the `configure network {ipv4 | ipv6} manual` command.

• **NTP**—Make sure the Firepower 4100 NTP server matches the FMC server set on the System > Configuration > Time Synchronization page.

• **Registration key, NAT ID, and FMC IP address**—Make sure you are using the same registration key, and if used, NAT ID, on both devices. You can set the registration key and NAT ID on the FTD using the `configure manager add` command. This command also lets you change the FMC IP address.
Configure a Basic Security Policy

This section describes how to configure a basic security policy with the following settings:

- Inside and outside interfaces—Assign a static IP address to the inside interface, and use DHCP for the outside interface.
- DHCP server—Use a DHCP server on the inside interface for clients.
- Default route—Add a default route through the outside interface.
- NAT—Use interface PAT on the outside interface.
- Access control—Allow traffic from inside to outside.

To configure a basic security policy, complete the following tasks.

1. Configure Interfaces, on page 63.
2. Configure the DHCP Server, on page 66.
3. Add the Default Route, on page 67.
4. Configure NAT, on page 68.
5. Allow Traffic from Inside to Outside, on page 71.
6. Deploy the Configuration, on page 72.

Configure Interfaces

Enable FTD interfaces, assign them to security zones, and set the IP addresses. Typically, you must configure at least a minimum of two interfaces to have a system that passes meaningful traffic. Normally, you would have an outside interface that faces the upstream router or internet, and one or more inside interfaces for your organization’s networks. Some of these interfaces might be “demilitarized zones” (DMZs), where you place publically-accessible assets such as your web server.

A typical edge-routing situation is to obtain the outside interface address through DHCP from your ISP, while you define static addresses on the inside interfaces.

The following example configures a routed mode inside interface with a static address and a routed mode outside interface using DHCP.

Procedure

**Step 1** Choose Devices > Device Management, and click the edit icon (✏️) for the device.
Step 2  
Click Interfaces.

![Interfaces tab](image)

Step 3  
Click the edit icon (📝) for the interface that you want to use for inside.

The General tab appears.

![Edit Physical Interface](image)

a) Enter a Name up to 48 characters in length.
   
   For example, name the interface inside.

b) Check the Enabled check box.

c) Leave the Mode set to None.

d) From the Security Zone drop-down list, choose an existing inside security zone or add a new one by clicking New.

   For example, add a zone called inside_zone. Each interface must be assigned to a security zone and/or interface group. An interface can belong to only one security zone, but can also belong to multiple interface groups. You apply your security policy based on zones or groups. For example, you can assign the inside interface to the inside zone; and the outside interface to the outside zone. Then you can configure your access control policy to enable traffic to go from inside to outside, but not from outside to inside. Most
policies only support security zones; you can use zones or interface groups in NAT policies, prefILTER policies, and QoS policies.

e) Click the IPv4 and/or IPv6 tab.

- IPv4—Choose Use Static IP from the drop-down list, and enter an IP address and subnet mask in slash notation.

For example, enter 192.168.1.1/24

- IPv6—Check the Autoconfiguration check box for stateless autoconfiguration.

f) Click OK.

**Step 4**

Click the edit icon (🔗) for the interface that you want to use for outside.

The General tab appears.

a) Enter a Name up to 48 characters in length.

For example, name the interface outside.

b) Check the Enabled check box.

c) Leave the Mode set to None.
d) From the Security Zone drop-down list, choose an existing outside security zone or add a new one by clicking New.

For example, add a zone called outside_zone.

e) Click the IPv4 and/or IPv6 tab.

- **IPv4**—Choose Use DHCP, and configure the following optional parameters:
  - **Obtain default route using DHCP**—Obtains the default route from the DHCP server.
  - **DHCP route metric**—Assigns an administrative distance to the learned route, between 1 and 255. The default administrative distance for the learned routes is 1.

- **IPv6**—Check the Autoconfiguration check box for stateless autoconfiguration.

f) Click OK.

**Step 5**

Click Save.

---

**Configure the DHCP Server**

Enable the DHCP server if you want clients to use DHCP to obtain IP addresses from the FTD.

**Procedure**

**Step 1**

Choose Devices > Device Management, and click the edit icon (-pencil) for the device.

**Step 2**

Choose DHCP > DHCP Server.

**Step 3**

On the Server page, click Add, and configure the following options:

- **Interface**—Choose the interface from the drop-down list.
• **Address Pool**—Set the range of IP addresses from lowest to highest that are used by the DHCP server. The range of IP addresses must be on the same subnet as the selected interface and cannot include the IP address of the interface itself.

• **Enable DHCP Server**—Enable the DHCP server on the selected interface.

**Step 4**  
Click **OK**.

**Step 5**  
Click **Save**.

---

### Add the Default Route

The default route normally points to the upstream router reachable from the outside interface. If you use DHCP for the outside interface, your device might have already received a default route. If you need to manually add the route, complete this procedure. If you received a default route from the DHCP server, it will show in the **IPv4 Routes** or **IPv6 Routes** table on the **Devices > Device Management > Routing > Static Route** page.

**Procedure**

**Step 1**  
Choose **Devices > Device Management**, and click the edit icon (📝) for the device.

**Step 2**  
Choose **Routing > Static Route**, click **Add Route**, and set the following:

- **Type**—Click the **IPv4** or **IPv6** radio button depending on the type of static route that you are adding.

- **Interface**—Choose the egress interface; typically the outside interface.
Configure NAT

- **Available Network**—Choose `any-ipv4` for an IPv4 default route, or `any-ipv6` for an IPv6 default route and click **Add** to move it to the **Selected Network** list.

- **Gateway** or **IPv6 Gateway**—Enter or choose the gateway router that is the next hop for this route. You can provide an IP address or a Networks/Hosts object.

- **Metric**—Enter the number of hops to the destination network. Valid values range from 1 to 255; the default value is 1.

**Step 3**

Click **OK**.

The route is added to the static route table.

**Step 4**

Click **Save**.

---

Configure NAT

A typical NAT rule converts internal addresses to a port on the outside interface IP address. This type of NAT rule is called *interface Port Address Translation (PAT)*.

**Procedure**

**Step 1**

Choose **Devices** > **NAT**, and click **New Policy** > **Threat Defense NAT**.

**Step 2**

Name the policy, select the device(s) that you want to use the policy, and click **Save**.
The policy is added the FMC. You still have to add rules to the policy.

**Step 3**  
Click Add Rule.

The Add NAT Rule dialog box appears.

**Step 4**  
Configure the basic rule options:

- **NAT Rule**—Choose Auto NAT Rule.
- **Type**—Choose Dynamic.

**Step 5**  
On the Interface Objects page, add the outside zone from the Available Interface Objects area to the Destination Interface Objects area.
Step 6  On the Translation page, configure the following options:

- **Original Source**—Click the add icon (🔗) to add a network object for all IPv4 traffic (0.0.0.0/0).

  ![Network Object Configuration](image)

  **Note**  You cannot use the system-defined *any-ipv4* object, because Auto NAT rules add NAT as part of the object definition, and you cannot edit system-defined objects.

- **Translated Source**—Choose Destination Interface IP.
Step 7 Click **Save** to add the rule.

The rule is saved to the **Rules** table.

Step 8 Click **Save** on the NAT page to save your changes.

## Allow Traffic from Inside to Outside

If you created a basic **Block all traffic** access control policy when you registered the FTD with the FMC, then you need to add rules to the policy to allow traffic through the device. The following procedure adds a rule to allow traffic from the inside zone to the outside zone. If you have other zones, be sure to add rules allowing traffic to the appropriate networks.

See the [FMC configuration guide](#) to configure more advanced security settings and rules.

### Procedure

**Step 1** Choose **Policy** > **Access Policy** > **Access Policy**, and click the edit icon (📝) for the access control policy assigned to the FTD.

**Step 2** Click **Add Rule**, and set the following parameters:

- **Name**—Name this rule, for example, **inside_to_outside**.
- **Source Zones**—Select the inside zone from **Available Zones**, and click **Add to Source**.
- **Destination Zones**—Select the outside zone from **Available Zones**, and click **Add to Destination**.
Leave the other settings as is.

**Step 3**  
Click **Add**.

The rule is added to the **Rules** table.

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

---

**Deploy the Configuration**

Deploy the configuration changes to the FTD; none of your changes are active on the device until you deploy them.

**Procedure**

**Step 1**  
Click **Deploy** in the upper right.

**Step 2**  
Select the device in the **Deploy Policies** dialog box, then click **Deploy**.

**Step 3**  
Ensure that the deployment succeeds. Click the icon to the right of the **Deploy** button in the menu bar to see status for deployments.
Access the Firepower Threat Defense CLI

You can use the FTD CLI to change management interface parameters and for troubleshooting purposes. You can access the CLI using SSH to the Management interface, or by connecting from the FXOS CLI.

**Procedure**

**Step 1** (Option 1) SSH directly to the FTD management interface IP address.

You set the management IP address when you deployed the logical device. Log into the FTD with the admin account and the password you set during initial deployment.

If you forgot the password, you can change it by editing the logical device in the Firepower Chassis Manager.

**Step 2** (Option 2) From the FXOS CLI, connect to the module CLI using a console connection or a Telnet connection.

a) Connect to the security engine.

\[\text{connect module 1 \{console | telnet\}}\]

The benefits of using a Telnet connection is that you can have multiple sessions to the module at the same time, and the connection speed is faster.

**Example:**

\[
\begin{align*}
\text{Firepower}\# &\text{ connect module 1 console} \\
\text{Telnet escape character is '}-'. \\
\text{Trying 127.5.1.1...} \\
\text{Connected to 127.5.1.1.} \\
\text{Escape character is '}-'. \\
\text{CISCO Serial Over LAN:} \\
\text{Close Network Connection to Exit} \\
\text{Firepower-module1>} \\
\end{align*}
\]

b) Connect to the FTD console.

\[\text{connect ftd name}\]
If you have multiple application instances, you must specify the name of the instance. To view the instance names, enter the command without a name.

**Example:**

```
Firepower-module1> connect ftd FTD_Instance1
```

You are connecting to ftd from a serial console. Please avoid executing any commands which may produce large amount of output. Otherwise, data cached along the pipe may take up to 12 minutes to be drained by a serial console at 9600 baud rate after pressing Ctrl-C.

To avoid the serial console, please login to FXOS with ssh and use 'connect module <slot> telnet' to connect to the security module.

Connecting to container ftd(FTD_Instance1) console... enter "exit" to return to bootCLI >

**c)** Exit the application console to the FXOS module CLI by entering **exit**.

**Note** For pre-6.3 versions, enter **Ctrl-a, d**.

d) Return to the supervisor level of the FXOS CLI.

**To exit the console:**

1. Enter ~
   
   You exit to the Telnet application.
   
2. To exit the Telnet application, enter:
   
   `telnet>quit`

**To exit the Telnet session:**

Enter **Ctrl-[, .**

**Example**

The following example connects to an FTD and then exits back to the supervisor level of the FXOS CLI.

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

CISCO Serial Over LAN:
Close Network Connection to Exit
```

```
Firepower-module1> connect ftd FTD_Instance1
```

---

Cisco Firepower 4100 Getting Started Guide

74
You are connecting to ftd from a serial console. Please avoid executing any commands which may produce large amount of output. Otherwise, data cached along the pipe may take up to 12 minutes to be drained by a serial console at 9600 baud rate after pressing Ctrl-C.

To avoid the serial console, please login to FXOS with ssh and use 'connect module <slot> telnet' to connect to the security module.

Connecting to container ftd(FTD_Instance1) console... enter "exit" to return to bootCLI
> ~
telnet> quit
Connection closed.
Firepower#

What's Next?

To continue configuring your FTD, see the documents available for your software version at Navigating the Cisco Firepower Documentation.

For information related to using FMC, see the Firepower Management Center Configuration Guide.

History for FTD with FMC

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Version</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for ASA and FTD on separate modules of the same Firepower 9300</td>
<td>6.4</td>
<td>You can now deploy ASA and FTD logical devices on the same Firepower 9300.</td>
</tr>
<tr>
<td>Note</td>
<td></td>
<td>Requires FXOS 2.6.1.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Version</td>
<td>Feature Information</td>
</tr>
<tr>
<td>--------------</td>
<td>---------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Multi-instance capability for Firepower Threat Defense on the Firepower 4100/9300</td>
<td>6.3.0</td>
<td>You can now deploy multiple logical devices, each with a Firepower Threat Defense container instance, on a single security engine/module. Formerly, you could only deploy a single native application instance. To provide flexible physical interface use, you can create VLAN subinterfaces in FXOS and also share interfaces between multiple instances. Resource management lets you customize performance capabilities for each instance. You can use High Availability using a container instance on 2 separate chassis. Clustering is not supported. <strong>Note</strong> Multi-instance capability is similar to ASA multiple context mode, although the implementation is different. Multiple context mode is not available on the Firepower Threat Defense.</td>
</tr>
</tbody>
</table>

New/Modified Firepower Management Center screens:
- **Devices > Device Management > Edit** icon > **Interfaces** tab

New/Modified Firepower Chassis Manager screens:
- **Overview > Devices**
- **Interfaces > All Interfaces > Add New** drop-down menu > **Subinterface**
- **Interfaces > All Interfaces > Type**
- **Logical Devices > Add Device**
- **Platform Settings > Mac Pool**
- **Platform Settings > Resource Profiles**
ASA Deployment

Is This Chapter for You?
This chapter describes how to deploy a standalone ASA logical device, including how to configure smart licensing. This chapter does not cover the following deployments, for which you should refer to the ASA configuration guide:

• Clustering
• Failover
• CLI configuration

This chapter also walks you through configuring a basic security policy; if you have more advanced requirements, refer to the configuration guide.

Privacy Collection Statement—The Firepower 4100 does not require or actively collect personally-identifiable information. However, you can use personally-identifiable information in the configuration, for example for usernames. In this case, an administrator might be able to see this information when working with the configuration or when using SNMP.

Note

• About the ASA, on page 77
• End-to-End Procedure, on page 78
• Firepower Chassis Manager: Register the Chassis with the Licensing Server, on page 79
• Firepower Chassis Manager: Add an ASA Logical Device, on page 83
• Log Into ASDM, on page 86
• Configure License Entitlements on the ASA, on page 87
• Configure the ASA, on page 88
• Access the ASA CLI, on page 89
• What's Next?, on page 90
• History for the ASA, on page 91

About the ASA
The ASA provides advanced stateful firewall and VPN concentrator functionality in one device. You can manage the ASA using one of the following managers:
- ASDM—A single device manager included on the device. This guide describes how to manage the ASA using ASDM.
- CLI
- Cisco Security Manager—A multi-device manager on a separate server.

**End-to-End Procedure**

See the following tasks to deploy and configure the ASA on your chassis.

1. Obtain feature licenses
2. Generate a license token for the chassis
3. Register the chassis with the Smart Licensing Server
4. Add an ASA logical device
5. Log into ASDM
6. Configure licenses on the ASA
7. Run wizards to configure the ASA

<table>
<thead>
<tr>
<th>Step</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cisco Commerce Workspace</td>
<td>Firepower Chassis Manager: Register the Chassis with the Licensing Server, on page 79: Obtain feature licenses.</td>
</tr>
<tr>
<td>2</td>
<td>Smart Software Manager</td>
<td>Firepower Chassis Manager: Register the Chassis with the Licensing Server, on page 79: Generate a license token for the chassis.</td>
</tr>
<tr>
<td>3</td>
<td>Firepower Chassis Manager</td>
<td>Firepower Chassis Manager: Register the Chassis with the Licensing Server, on page 79: Register the chassis with the Smart Licensing server.</td>
</tr>
</tbody>
</table>
Firepower Chassis Manager: Register the Chassis with the Licensing Server

The ASA uses Cisco Smart Software Licensing. You can use regular Smart Software Licensing, which requires internet access; or for offline management, you can configure Permanent License Reservation or a Satellite server. For more information about these offline licensing methods, see Cisco ASA Series Feature Licenses; this guide applies to regular Smart Software Licensing.

For the ASA on the Firepower 4100, Smart Software Licensing configuration is split between FXOS on the chassis and the ASA.

- Firepower 4100—Configure all Smart Software Licensing infrastructure in FXOS, including parameters for communicating with the License Authority. The Firepower 4100 itself does not require any licenses to operate.

- ASA—Configure all license entitlements in the ASA.

When you register the chassis, the License Authority issues an ID certificate for communication between the chassis and the License Authority. It also assigns the chassis to the appropriate virtual account. Until you register with the License Authority, you will not be able to make configuration changes to features requiring special licenses, but operation is otherwise unaffected. Licensed features include:

- Standard
- Security Contexts
- Carrier—Diameter, GTP/GPRS, SCTP
- Strong Encryption (3DES/AES)
- AnyConnect—AnyConnect Plus, AnyConnect Apex, or AnyConnect VPN Only.

When you request the registration token for the ASA from your Smart Software Licensing account, check the Allow export-controlled functionality on the products registered with this token check box so that the full Strong Encryption license is applied (your account must be qualified for its use). The Strong Encryption license is automatically enabled for qualified customers when you apply the registration token on the chassis, so no additional action is required.

Strong encryption is required for ASDM access.
Before you begin

- Have a master account on the Cisco Smart Software Manager. 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.

- Your Cisco Smart Software Licensing account must qualify for the Strong Encryption (3DES/AES) license to use some features (enabled using the export-compliance flag).

- If you have not already done so, Configure NTP, on page 10.

- If you did not configure DNS during the initial setup, add a DNS server on the Platform Settings > DNS page.

Procedure

Step 1
Make sure your Smart Licensing account contains the available licenses you need, including at a minimum the Standard license.

When you bought your device from Cisco or a reseller, your licenses should have been linked to your Smart Software License account. However, if you need to add licenses yourself, use the Find Products and Solutions search field on the Cisco Commerce Workspace. Search for the following license PIDs:

Figure 5: License Search

- Standard license—L-FPR4100-ASA=. The Standard license is free, but you still need to add it to your Smart Software Licensing account.

- 10 context license—L-FPR4K-ASASC-10=. Context licenses are additive; buy multiple licenses to meet your needs.

- 230 context license—L-FPR4K-ASASC-230=. Context licenses are additive; buy multiple licenses to meet your needs.

- 250 context license—L-FPR4K-ASASC-250=. Context licenses are additive; buy multiple licenses to meet your needs.

- Carrier (Diameter, GTP/GPRS, SCTP)—L-FPR4K-ASA-CAR=

- Strong Encryption (3DES/AES) license—L-FPR4K-ENC-K9=. This license is free. Although this license is not generally required (for example, ASAs that use older Satellite Server versions (pre-2.3.0) require this license), you should still add it to your account for tracking purposes.

- Anyconnect—See the Cisco AnyConnect Ordering Guide. You do not enable this license directly in the ASA.
Step 2  In the Cisco Smart Software Manager, request and copy a registration token for the virtual account to which you want to add this device.

a) Click Inventory.

![Inventory button highlighted](Image)


![New Token button highlighted](Image)

c) On the Create Registration Token dialog box enter the following settings, and then click Create Token:

![Create Registration Token dialog box](Image)

- **Description**
- **Expire After**—Cisco recommends 30 days.
- **Allow export-controlled functionality on the products registered with this token**—Enables the export-compliance flag.

The token is added to your inventory.

d) Click the arrow icon to the right of the token to open the Token dialog box so you can copy the token ID to your clipboard. Keep this token ready for later in the procedure when you need to register the ASA.
Step 3  In the Firepower Chassis Manager, choose System > Licensing > Smart License.

Step 4  Enter the registration token in the Enter Product Instance Registration Token field.

Step 5  Click Register.

The Firepower 4100 registers with the License Authority. Successful registration can take several minutes. Refresh this page to see the status.
Firepower Chassis Manager: Add an ASA Logical Device

You can deploy an ASA from the Firepower 4100 as a native instance.

To add a failover pair or cluster, see the ASA general operations configuration guide.

This procedure lets you configure the logical device characteristics, including the bootstrap configuration used by the application.

Before you begin

- Configure a Management interface to use with the ASA; see Configure Interfaces, on page 14. The Management interface is required. Note that this Management interface is not the same as the chassis management port that is used only for chassis management (and that appears at the top of the Interfaces tab as MGMT).

- Gather the following information:
  - Interface IDs for this device
  - Management interface IP address and network mask
  - Gateway IP address
  - New admin password/enable password

Procedure

Step 1 In Firepower Chassis Manager, choose Logical Devices.

Step 2 Click Add > Standalone, and set the following parameters:
a) Provide a **Device Name**.

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

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

c) Choose the **Image Version**.

d) Click **OK**.

You see the Provisioning - *device name* window.

**Step 3**

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

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

**Step 4**

Click the device icon in the center of the screen.

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

**Step 5**

On the **General Information** page, complete the following:
a) Choose the **Management Interface**.
   This interface is used to manage the logical device. This interface is separate from the chassis management port.

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

c) Configure the **Management IP address**.
   Set a unique IP address for this interface.

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

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

**Step 6**  
Click **Settings**.

a) Choose the **Firewall Mode**: Routed or Transparent.
   In routed mode, the ASA is considered to be a router hop in the network. Each interface that you want to route between is on a different subnet. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a “bump in the wire,” or a “stealth firewall,” and is not seen as a router hop to connected devices.
   The firewall mode is only set at initial deployment. If you re-apply the bootstrap settings, this setting is not used.

b) Enter and confirm a **Password** for the admin user and for the enable password.
   The preconfigured ASA admin user/password and enable password are useful for password recovery; if you have FXOS access, then you can reset the admin user password/enable password if you forget it.
Log Into ASDM

Launch ASDM so you can configure the ASA.

Before you begin

- See the ASDM release notes on Cisco.com for the requirements to run ASDM.
- Make sure the ASA logical device Status is online on the Firepower Chassis Manager Logical Devices page.

Procedure

Step 1 Enter the following URL in your browser.

  - https://management_ip—Management interface IP address that you entered in the bootstrap configuration.

  The Cisco ASDM web page appears. You may see browser security warnings because the ASA does not have a certificate installed; you can safely ignore these warnings and visit the web page.

Step 2 Click one of these available options: Install ASDM Launcher or Run ASDM.

Step 3 Follow the onscreen instructions to launch ASDM according to the option you chose.

  The Cisco ASDM-IDM Launcher appears.

Step 4 Leave the username empty, enter the enable password that you set when you deployed the ASA, and click OK.
The main ASDM window appears.

## Configure License Entitlements on the ASA

Assign licenses to the ASA. You must at a minimum assign the Standard license.

**Before you begin**

- Firepower Chassis Manager: Register the Chassis with the Licensing Server, on page 79.

**Procedure**

**Step 1**
In ASDM, choose Configuration > Device Management > Licensing > Smart Licensing.

**Step 2**
Set the following parameters:

- **a)** Check Enable Smart license configuration.
- **b)** From the Feature Tier drop-down list, choose Standard.
  
  Only the Standard tier is available.

- **c)** (Optional) For the Context license, enter the number of contexts.
  
  You can use 10 contexts without a license. The maximum number of contexts is 250. For example, to use the maximum, enter 240 for the number of contexts; this value is added to the default of 10.

- **d)** (Optional) Check Carrier.

**Step 3**
(Optional) The Enable strong-encryption protocol is generally not required; for example, ASAs that use older Satellite Server versions (pre-2.3.0) require this license, but you can check this box if you know you need to, or if you want to track usage of this license in your account.

**Step 4**
Click Apply.

If you do not have the appropriate licenses in your account, you cannot apply your license changes.

**Step 5**
Click the Save icon in the toolbar.

**Step 6**
Quit ASDM and relaunch it.
When you change licenses, you need to relaunch ASDM to show updated screens.

Configure the ASA

Using ASDM, you can use wizards to configure basic and advanced features. You can also manually configure features not included in wizards.

Procedure

**Step 1** Choose Wizards > Startup Wizard, and click the Modify existing configuration radio button.

**Step 2** The Startup Wizard walks you through configuring:
• The enable password
• Interfaces, including setting the inside and outside interface IP addresses and enabling interfaces.
• Static routes
• The DHCP server
• And more...

Step 3 (Optional) From the Wizards menu, run other wizards.
Step 4 To continue configuring your ASA, see the documents available for your software version at Navigating the Cisco ASA Series Documentation.

Access the ASA CLI

You can use the ASA CLI to troubleshoot or configure the ASA instead of using ASDM. You can access the CLI by connecting from the FXOS CLI. You can later configure SSH access to the ASA on any interface. See the ASA general operations configuration guide for more information.

Procedure

Step 1 From the FXOS CLI, connect to the module CLI using a console connection or a Telnet connection.

```
connect module 1 {console | telnet}
```

The benefits of using a Telnet connection is that you can have multiple sessions to the module at the same time, and the connection speed is faster.

Example:

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

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

Step 2 Connect to the ASA console.

```
connect asa
```

Example:

```
Firepower-module1> connect asa
Connecting to asa(asal) console... hit Ctrl + A + D to return to bootCLI
[...] asa>
```
Step 3
Exit the application console to the FXOS module CLI by entering Ctrl-a, d.

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

Exit the console:

a) Enter ~
   You exit to the Telnet application.

b) To exit the Telnet application, enter:
   telnet>quit

Exit the Telnet session:

a) Enter Ctrl-[], .

Example

The following example shows how to connect to an ASA and then exit back to the supervisor level of the FXOS CLI.

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

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect asa
asa> ~
telnet> quit
Connection closed.
Firepower#

What's Next?

• To continue configuring your ASA, see the documents available for your software version at Navigating the Cisco ASA Series Documentation.
## History for the ASA

<table>
<thead>
<tr>
<th>Feature</th>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for ASA and FTD on separate modules of the same Firepower 9300</td>
<td>9.12(1)</td>
<td>You can now deploy ASA and FTD logical devices on the same Firepower 9300.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> Requires FXOS 2.6.1.</td>
</tr>
<tr>
<td>Support for transparent mode deployment for an ASA logical device</td>
<td>9.10(1)</td>
<td>You can now specify transparent or routed mode when you deploy the ASA.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> Requires FXOS 2.4.1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>New/modified Firepower Chassis Manager screens:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Logical Devices</strong> &gt; <strong>Add Device</strong> &gt; <strong>Settings</strong> &gt; <strong>Firewall Mode</strong> drop-down list</td>
</tr>
<tr>
<td>Smart Agent Upgrade to v1.6</td>
<td>9.6(2)</td>
<td>The smart agent was upgraded from Version 1.1 to Version 1.6. This upgrade supports permanent license reservation and also supports setting the Strong Encryption (3DES/AES) license entitlement according to the permission set in your license account.</td>
</tr>
<tr>
<td>New Carrier license</td>
<td>9.5(2)</td>
<td>The new Carrier license replaces the existing GTP/GPRS license, and also includes support for SCTP and Diameter inspection. For the ASA on the Firepower 9300, the <code>feature mobile-sp</code> command will automatically migrate to the <code>feature carrier</code> command. We modified the following screen: <strong>Configuration</strong> &gt; <strong>Device Management</strong> &gt; <strong>Licensing</strong> &gt; <strong>Smart License</strong></td>
</tr>
</tbody>
</table>