Firepower Threat Defense Deployment with FDM

Note Firepower version 7.0 is the final supported version for the ASA 5508-X and 5516-X.

Is This Chapter for You?

This chapter explains how to complete the initial set up and configuration of your Firepower Threat Defense (FTD) device using the Firepower Device Manager (FDM) web-based device setup wizard.

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.

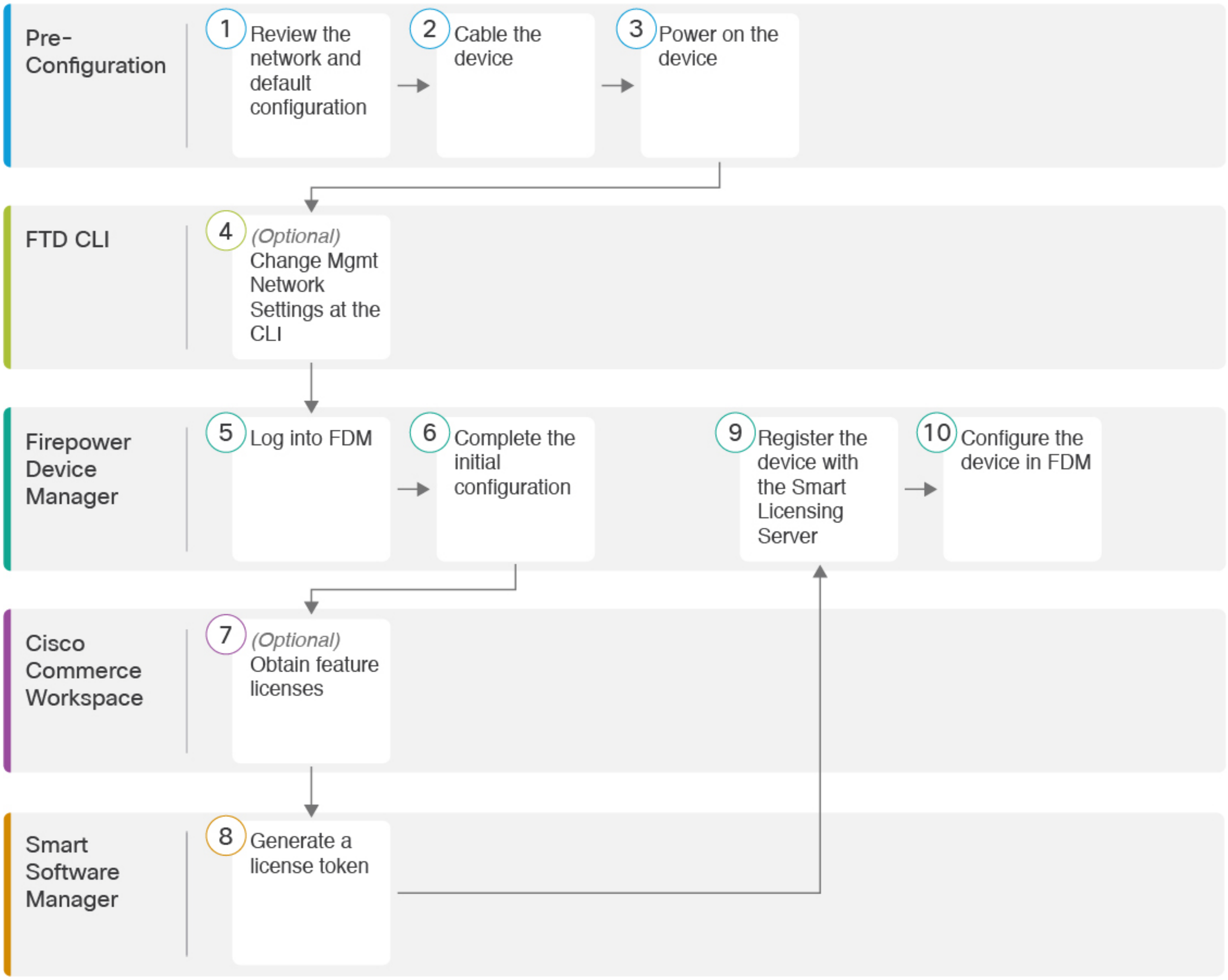
If you are managing large numbers of devices, or if you want to use the more complex features and configurations that FTD allows, use the Firepower Management Center (FMC) instead.

The Cisco ASA 5508-X and 5516-X hardware can run either FTD software or ASA software. Switching between FTD and ASA requires you to reimage the device. See Reimage the Cisco ASA or Firepower Threat Defense Device.

Privacy Collection Statement—The ASA 5508-X and 5516-X 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.

End-to-End Procedure

See the following tasks to deploy FTD with FDM on your chassis.


Pre-Configuration
1 Review the network and default configuration
2 Cable the device
3 Power on the device
FTD CLI
4 (Optional) Change Mgmt Network Settings at the CLI
Firepower Device Manager
5 Log into FDM
6 Complete the initial configuration
9 Register the device with the Smart Licensing Server
10 Configure the device in FDM
Cisco Commerce Workspace
7 (Optional) Obtain feature licenses
Smart Software Manager
8 Generate a license token

1	Pre-Configuration	Review the Network Deployment and Default Configuration, on page 3.
2	Pre-Configuration	Cable the Device, on page 5
3	Pre-Configuration	Power on the Device, on page 6.

4	FTD CLI	(Optional) Change Management Network Settings at the CLI, on page 7.
5	Firepower Device Manager	Log Into FDM, on page 9.
6	Firepower Device Manager	Complete the Initial Configuration, on page 9.
7	Cisco Commerce Workspace	Configure Licensing, on page 11: Obtain license features.
8	Smart Software Manager	Configure Licensing, on page 11: Generate a license token.
9	Firepower Device Manager	Configure Licensing, on page 11: Register the device with the Smart Licensing Server.
10	Firepower Device Manager	Configure the Firewall in Firepower Device Manager, on page 17.

Review the Network Deployment and Default Configuration

You can manage the FTD using FDM from either the Management 1/1 interface or the inside interface. The dedicated Management interface is a special interface with its own network settings.

The following figure shows the recommended network deployment. If you connect the outside interface directly to a cable modem or DSL modem, we recommend that you put the modem into bridge mode so the FTD performs all routing and NAT for your inside networks. If you need to configure PPPoE for the outside interface to connect to your ISP, you can do so after you complete initial setup in FDM.

Note

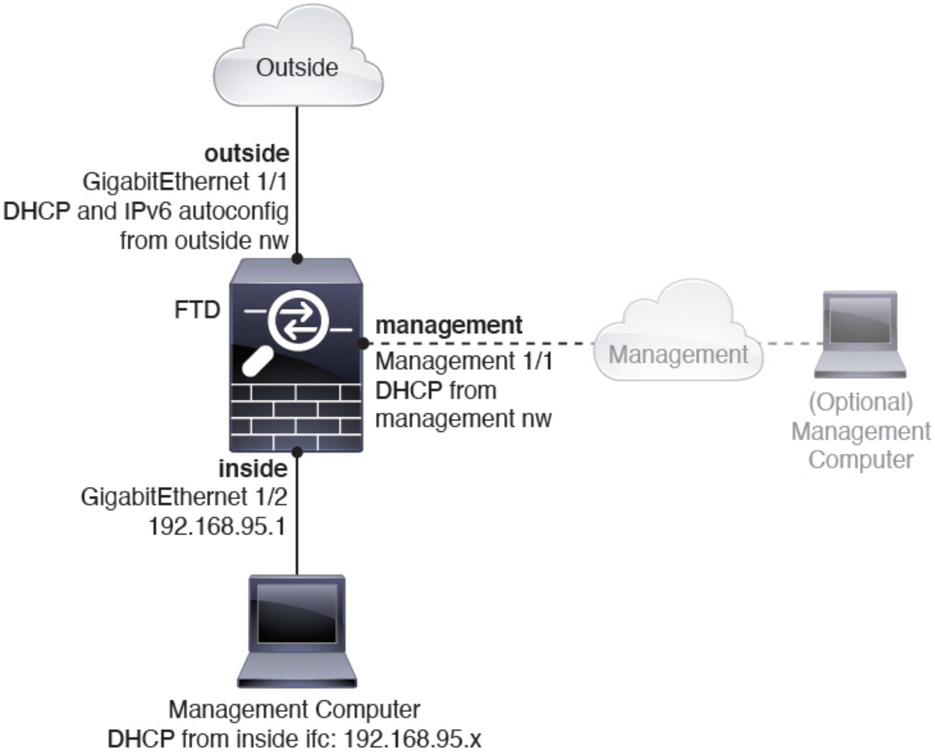
If you cannot use the default management IP address (for example, your management network does not include a DHCP server), then you can connect to the console port and perform initial setup at the CLI, including setting the Management IP address, gateway, and other basic networking settings.

If you need to change the inside IP address, you can do so after you complete initial setup in FDM. For example, you may need to change the inside IP address in the following circumstances:

- (7.0 and later) The inside IP address is 192.168.95.1. (6.7 and earlier) The inside IP address is 192.168.1.1. If the outside interface tries to obtain an IP address on the 192.168.1.0 network, which is a common default network, the DHCP lease will fail, and the outside interface will not obtain an IP address. This problem occurs because the FTD cannot have two interfaces on the same network. In this case you must change the inside IP address to be on a new network.
- If you add the FTD to an existing inside network, you will need to change the inside IP address to be on the existing network.

The following figure shows the default network deployment for FTD using FDM with the default configuration.

Figure 1: Suggested Network Deployment



Note For 6.7 and earlier, the GigabitEthernet 1/2 inside IP address is 192.168.1.1.

For 6.5 and earlier, the Management 1/1 default IP address is 192.168.45.45.

Default Configuration

The configuration for the f after initial setup includes the following:

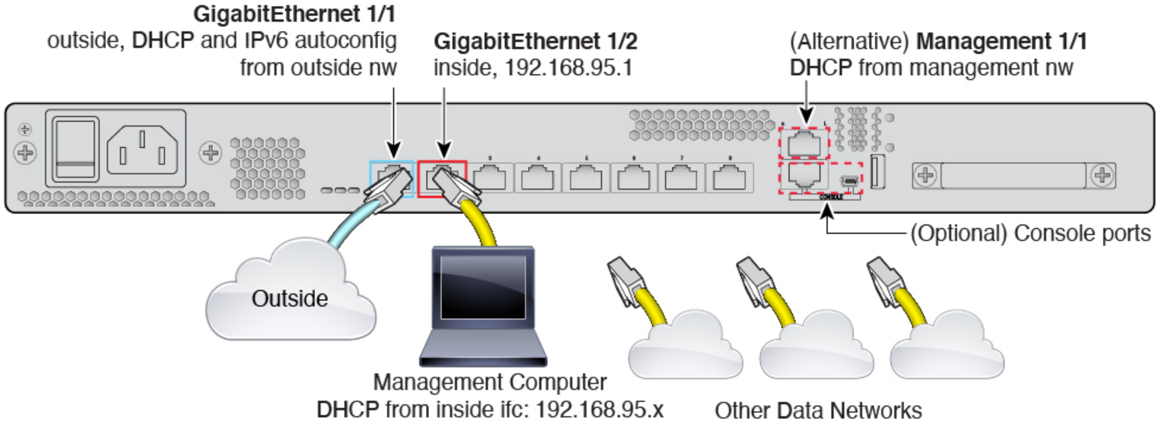
- **inside**—GigabitEthernet 1/2, IP address (7.0 and later) 192.168.95.1; (pre-7.0) 192.168.1.1.
- **outside**—Ethernet 1/1, IP address from IPv4 DHCP and IPv6 autoconfiguration
- **inside→outside** traffic flow
- **management**—Management 1/1 (management)
  - (6.6 and later) IP address from DHCP
  - (6.5 and earlier) IP address 192.168.45.45

Note The Management 1/1 interface is a special interface separate from data interfaces that is used for management, Smart Licensing, and database updates. The physical interface is shared with a second logical interface, the Diagnostic interface. Diagnostic is a data interface, but is limited to other types of management traffic (to-the-device and from-the-device), such as syslog or SNMP. The Diagnostic interface is not typically used. See the FDM configuration guide for more information.

- **DNS server for management**—OpenDNS: (IPv4) 208.67.222.222, 208.67.220.220; (IPv6) 2620:119:35::35, or servers you specify during setup. DNS servers obtained from DHCP are never used.
- **NTP**—Cisco NTP servers: 0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org, or servers you specify during setup
- **Default routes**
  - **Data interfaces**—Obtained from outside DHCP, or a gateway IP address you specify during setup
  - **Management interface**—(6.6 and later) Obtained from management DHCP. If you do not receive a gateway, then the default route is over the backplane and through the data interfaces. (6.5 and earlier) Over the backplane and through the data interfaces

    Note that the Management interface requires internet access for licensing and updates, either over the backplane or using a separate internet gateway. Note that only traffic originating on the Management interface can go over the backplane; otherwise, Management does not allow through traffic for traffic entering Management from the network.
- **DHCP server**—Enabled on the inside interface and (6.5 and earlier only) management interface
- **FDM access**—All hosts allowed on Management and inside interfaces.
- **NAT**—Interface PAT for all traffic from inside to outside

Cable the Device



Note For 6.7 and earlier, the GigabitEthernet 1/2 inside IP address is 192.168.1.1.

For 6.5 and earlier, the Management 1/1 default IP address is 192.168.45.45.

Manage the ASA 5508-X or 5516-X on either Management 1/1 or GigabitEthernet 1/2. The default configuration also configures GigabitEthernet 1/1 as outside.

Procedure

Step 1 Connect your management computer to one of the following interfaces:

- GigabitEthernet 1/2—Connect your management computer directly to GigabitEthernet 1/2 for initial configuration, or connect GigabitEthernet 1/2 to your inside network. GigabitEthernet 1/2 has a default IP address (192.168.95.1) and also runs a DHCP server to provide IP addresses to clients (including the management computer), so make sure these settings do not conflict with any existing inside network settings
- Management 1/1—Connect your management computer to the management network. The Management 1/1 interface obtains an IP address from DHCP, so make sure your network includes a DHCP server.

  If you need to change the Management 1/1 IP address from the default to configure a static IP address, you must also cable your management PC to the console port. See (Optional) Change Management Network Settings at the CLI, on page 7.

You can later configure FDM management access from other interfaces; see the FDM configuration guide.

Step 2 Connect the outside network to the GigabitEthernet 1/1 interface.

By default, the IP address is obtained using IPv4 DHCP and IPv6 autoconfiguration, but you can set a static address during initial configuration.

Step 3 Connect other networks to the remaining interfaces.

Power on the Device

System power is controlled by a rocker power switch located on the rear of the device.

Before you begin

It's important that you provide reliable power for your device (for example, using an uninterruptable power supply (UPS)). Loss of power without first shutting down can cause serious file system damage. There are many processes running in the background all the time, and losing power does not allow the graceful shutdown of your system.

Procedure

Step 1 Attach the power cord to the device, and connect it to an electrical outlet.

Step 2 Turn the power on using the standard rocker-type power on/off switch located on the rear of the chassis, adjacent to the power cord.

Step 3 Check the Power LED on the front or rear of the device; if it is solid green, the device is powered on.

Figure 2: Rear Panel

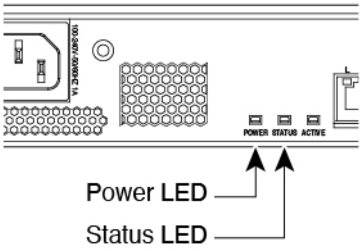
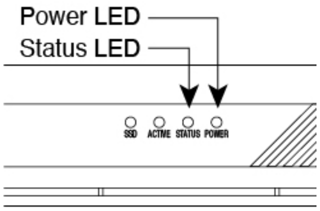


Figure 3: Front Panel



Step 4 Check the Status LED on the front or rear of the device; after it is solid green, the system has passed power-on diagnostics.

(Optional) Change Management Network Settings at the CLI

If you cannot use the default management IP address, then you can connect to the console port and perform initial setup at the CLI, including setting the Management IP address, gateway, and other basic networking settings. You can only configure the Management interface settings; you cannot configure inside or outside interfaces, which you can later configure in the GUI.

Note You cannot repeat the CLI setup script unless you clear the configuration; for example, by reimaging. However, all of these settings can be changed later at the CLI using **configure network** commands. See the threat defense command reference.

Procedure

Step 1 Connect to the FTD console port. See Access the Firepower Threat Defense CLI, on page 20 for more information.

Log in with the **admin** user and the default password, **Admin123**.

Note If the password was already changed, and you do not know it, you must reimage the device to reset the password to the default. See the reimage guide for instructions.

Step 2 The first time you log in to FTD, you are prompted to accept the End User License Agreement (EULA) and to change the admin password. You are then presented with the CLI setup script.

Defaults or previously-entered values appear in brackets. To accept previously entered values, press **Enter**.

See the following guidelines:

- **Enter the IPv4 default gateway for the management interface**—If you set a manual IP address, enter either **data-interfaces** or the IP address of the gateway router. The **data-interfaces** setting sends outbound management traffic over the backplane to exit a data interface. This setting is useful if you do not have a separate Management network that can access the internet. Traffic originating on the Management interface includes license registration and database updates that require internet access. If you use **data-interfaces**, you can still use the FDM (or SSH) on the Management interface if you are directly-connected to the Management network, but for remote management for specific networks or hosts, you should add a static route using the **configure network static-routes** command. Note that FDM management on data interfaces is not affected by this setting. If you use DHCP, the system uses the gateway provided by DHCP and uses the **data-interfaces** as a fallback method if DHCP doesn't provide a gateway.

- **If your networking information has changed, you will need to reconnect**—If you are connected with SSH to the default IP address but you change the IP address at initial setup, you will be disconnected. Reconnect with the new IP address and password. Console connections are not affected.

- **Manage the device locally?**—Enter **yes** to use the FDM or the CDO. A **no** answer means you intend to use the FMC to manage the device.

Example:

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must change the password for 'admin' to continue.
Enter new password: ********
Confirm new password: ********
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: yes

>
```

Step 3 Log into the FDM on the new Management IP address.

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.

Procedure

Step 1 Enter the following URL in your browser.

- (7.0 and later) Inside (GigabitEthernet 1/2)—**https://192.168.95.1**.
- (6.7 and earlier) Inside (GigabitEthernet 1/2)—**https://192.168.1.1**.
- (6.6 and later) Management—**https://***management_ip*. The Management interface is a DHCP client, so the IP address depends on your DHCP server. If you changed the Management IP address at the CLI setup, then enter that address.
- (6.5 and earlier) Management—**https://192.168.45.45**. If you changed the Management IP address at the CLI setup, then enter that address.

Step 2 Log in with the username **admin**, and thedefault password **Admin123**.

What to do next

- Run through the FDM setup wizard; see Complete the Initial Configuration, on page 9.

Complete the Initial Configuration

Use the setup wizard when you first log into FDM to complete the initial configuration. After you complete the setup wizard, you should have a functioning device with a few basic policies in place:

- An outside (GigabitEthernet1/1) and an inside interface (GigabitEthernet1/2).
- Security zones for the inside and outside interfaces.
- An access rule trusting all inside to outside traffic.
- An interface NAT rule that translates all inside to outside traffic to unique ports on the IP address of the outside interface.
- A DHCP server running on the inside interface.

Note If you performed the (Optional) Change Management Network Settings at the CLI, on page 7 procedure, then some of these tasks, specifically changing the admin password and configuring the outside and management interfaces, should have already been completed.

Procedure

Step 1 You are prompted to read and accept the End User License Agreement and change the admin password.

You must complete these steps to continue.

Step 2 Configure the following options for the outside and management interfaces and click **Next**.

Note Your settings are deployed to the device when you click **Next**. The interface will be named "outside" and it will be added to the "outside_zone" security zone. Ensure that your settings are correct.

a) **Outside Interface**—This is the data port that you connected to your gateway router. You cannot select an alternative outside interface during initial device setup. The first data interface is the default outside interface.

Configure IPv4—The IPv4 address for the outside interface. You can use DHCP or manually enter a static IP address, subnet mask, and gateway. You can also select **Off** to not configure an IPv4 address. You cannot configure PPPoE using the setup wizard. PPPoE may be required if the interface is connected to a DSL modem, cable modem, or other connection to your ISP, and your ISP uses PPPoE to provide your IP address. You can configure PPPoE after you complete the wizard.

Configure IPv6—The IPv6 address for the outside interface. You can use DHCP or manually enter a static IP address, prefix, and gateway. You can also select **Off** to not configure an IPv6 address.

b) **Management Interface**

DNS Servers—The DNS server for the system's management address. Enter one or more addresses of DNS servers for name resolution. The default is the OpenDNS public DNS servers. If you edit the fields and want to return to the default, click **Use OpenDNS** to reload the appropriate IP addresses into the fields.

Firewall Hostname—The hostname for the system's management address.

Step 3 Configure the system time settings and click **Next**.

a) **Time Zone**—Select the time zone for the system.
b) **NTP Time Server**—Select whether to use the default NTP servers or to manually enter the addresses of your NTP servers. You can add multiple servers to provide backups.

Step 4 (Optional) Configure the smart licenses for the system.

Your purchase of a Firepower Threat Defense device automatically includes a Base license. All additional licenses are optional.

You must have a smart license account to obtain and apply the licenses that the system requires. Initially, you can use the 90-day evaluation license and set up smart licensing later.

To register the device now, click the link to log into your Smart Software Manager account, and see Configure Licensing, on page 11.

To use the evaluation license, select **Start 90 day evaluation period without registration**.

Step 5 Click **Finish**.

What to do next

- Although you can continue using the evaluation license, we recommend that you register and license your device; see Configure Licensing, on page 11.
- You can also choose to configure the device using FDM; see Configure the Firewall in Firepower Device Manager, on page 17.

Configure Licensing

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

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

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide

The Base license is included automatically. Smart Licensing does not prevent you from using product features that you have not yet purchased. You can start using a license immediately, as long as you are registered with the Smart Software Manager, and purchase the license later. This allows you to deploy and use a feature, and avoid delays due to purchase order approval. See the following licenses:

- **Threat**—Security Intelligence and Next-Generation IPS
- **Malware**—Malware
- **URL**—URL Filtering
- **RA VPN**—AnyConnect Plus, AnyConnect Apex, or AnyConnect VPN Only

Before you begin

- Have a master account on the 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.

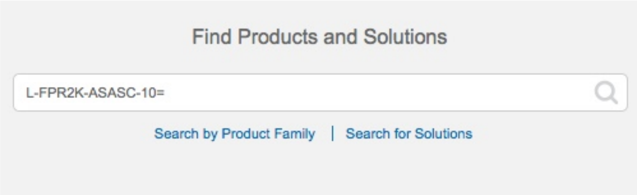
- Your Smart Software Licensing account must qualify for the Strong Encryption (3DES/AES) license to use some features (enabled using the export-compliance flag).

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 4: License Search



Find Products and Solutions
Search by Product Family | Search for Solutions

L-FPR2K-ASASC-10=

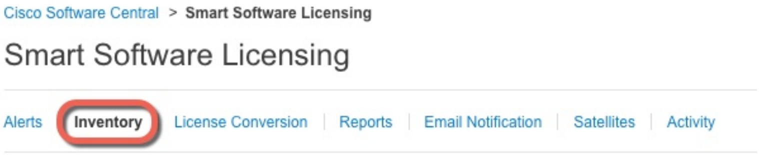
Note If a PID is not found, you can add the PID manually to your order.

- Threat, Malware, and URL license combination:
  - L-ASA5508T-TMC=
  - L-ASA5516T-TMC=

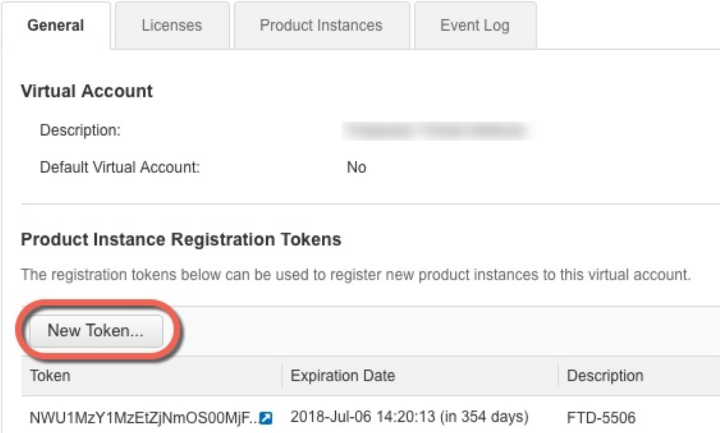
  When you add one of the above PIDs to your order, you can then choose a term-based subscription corresponding with one of the following PIDs:
  - L-ASA5508T-TMC-1Y
  - L-ASA5508T-TMC-3Y
  - L-ASA5508T-TMC-5Y
  - L-ASA5516T-TMC-1Y
  - L-ASA5516T-TMC-3Y
  - L-ASA5516T-TMC-5Y
- RA VPN—See the Cisco AnyConnect Ordering Guide.

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

a) Click **Inventory**.



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



Virtual Account

Description: [redacted]

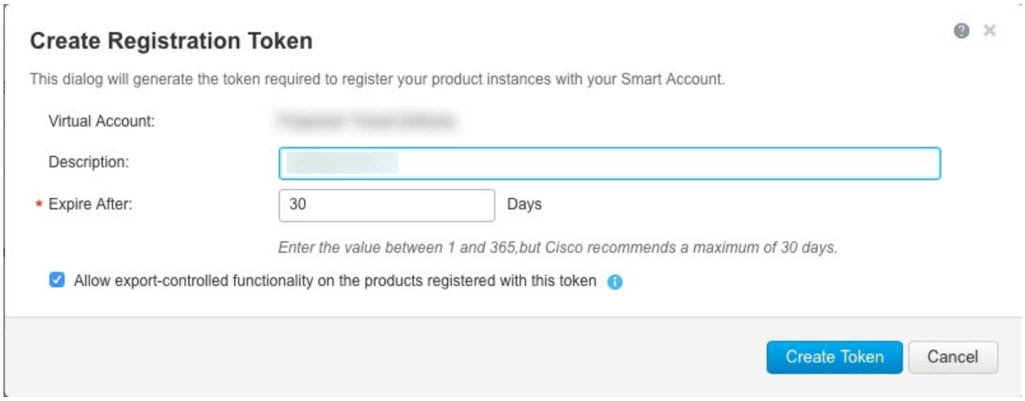
Default Virtual Account: No

Product Instance Registration Tokens

The registration tokens below can be used to register new product instances to this virtual account.

Token	Expiration Date	Description
NWU1MzY1MzEtZjNmOS00MjF..	2018-Jul-06 14:20:13 (in 354 days)	FTD-5506

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



Create Registration Token

This dialog will generate the token required to register your product instances with your Smart Account.

Virtual Account: [redacted]

Description: [redacted]

* Expire After: 30 Days

Enter the value between 1 and 365,but Cisco recommends a maximum of 30 days.

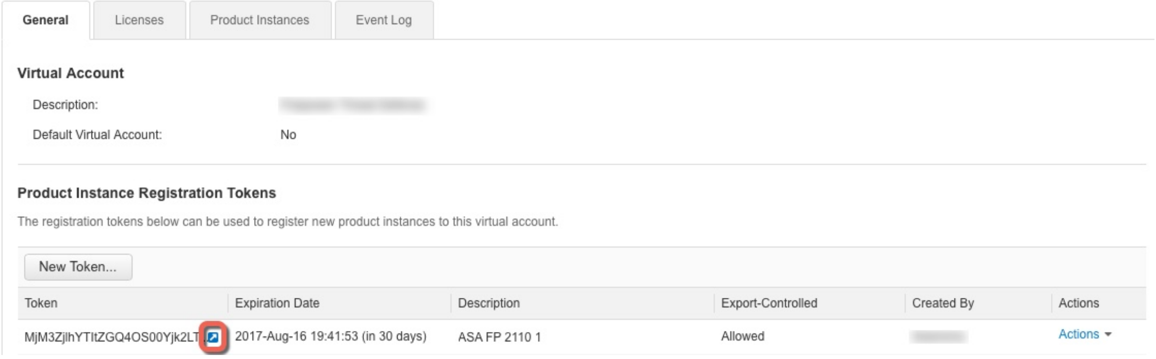
☑ Allow export-controlled functionality on the products registered with this token

- **Description**
- **Expire After**—Cisco recommends 30 days.
- **Allow export-controlled functionaility on the products registered with this token**—Enables the export-compliance flag if you are in a country that allows for strong encryption. You must select this option now if you plan to use this functionality. If you enable this functionality later, you will need to re-register your device with a new product key and reload the device. If you do not see this option, your account does not support export-controlled functionality.

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 5: View Token



General | Licenses | Product Instances | Event Log

Virtual Account

Description: [redacted]

Default Virtual Account: No

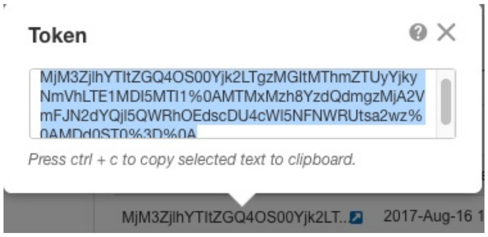
Product Instance Registration Tokens

The registration tokens below can be used to register new product instances to this virtual account.

New Token...

Token	Expiration Date	Description	Export-Controlled	Created By	Actions
MjM3ZjlhYTItZGQ4OS00Yjk2LT	2017-Aug-16 19:41:53 (in 30 days)	ASA FP 2110 1	Allowed	[redacted]	Actions

Figure 6: Copy Token



Token

MjM3ZjlhYTItZGQ4OS00Yjk2LTgzMGItMThmZTUyYjky
NmVhLTE1MDI5MTI1%0AMTMxMzh8YzdQdmgzMjA2V
mFJN2dYQjl5QWRhOEdscDU4cWI5NFNWRUtsa2wz%
0AMDd0ST0%3D%0A

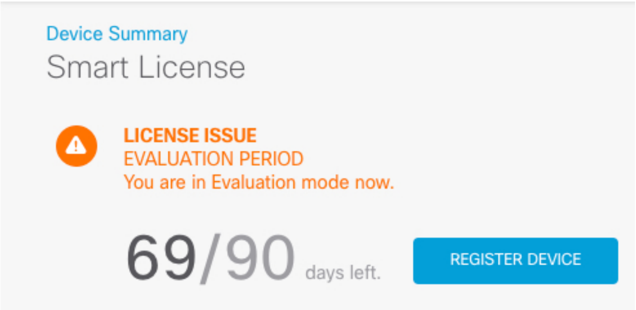
Press ctrl + c to copy selected text to clipboard.

MjM3ZjlhYTItZGQ4OS00Yjk2LT.. 2017-Aug-16 1

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

You see the **Smart License** page.

Step 4 Click **Register Device**.



Device Summary

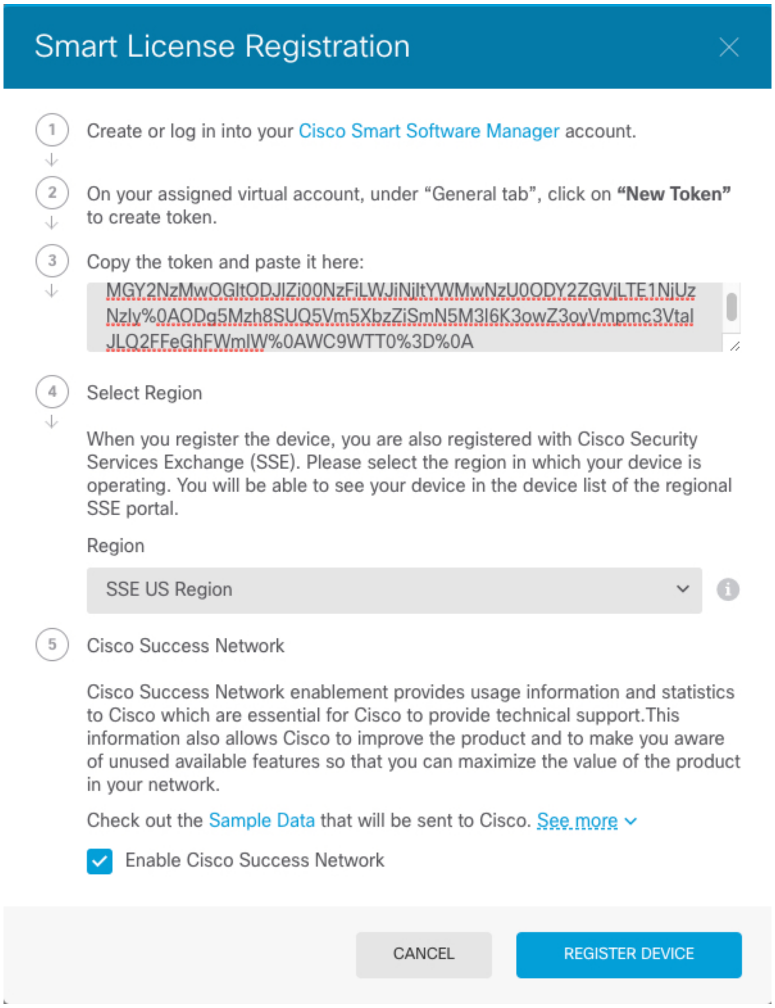
Smart License

LICENSE ISSUE
EVALUATION PERIOD
You are in Evaluation mode now.

69/90 days left.

REGISTER DEVICE

Then follow the instructions on the **Smart License Registration** dialog box to paste in your token:



Smart License Registration

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:

```
MGY2NzMwOGltODJlZi00NzFiLWJiNjltYWMwNzU0ODY2ZGVjLTE1NjUz
Nzly%0AODg5Mzh8SUQ5Vm5XbzZiSmN5M3l6K3owZ3oyVmpmc3Vtal
JLQ2FFeGhFWmlW%0AWC9WTT0%3D%0A
```

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.

Region

SSE US Region

5 Cisco Success Network

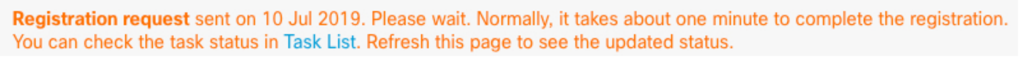
Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support.This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.

Check out the Sample Data that will be sent to Cisco. See more

☑ Enable Cisco Success Network

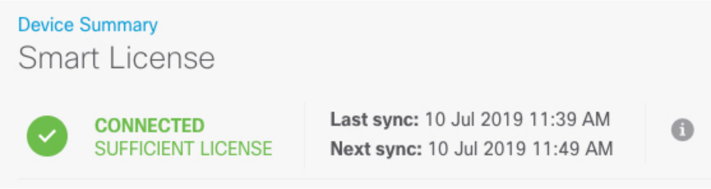
Step 5 Click **Register Device**.

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:



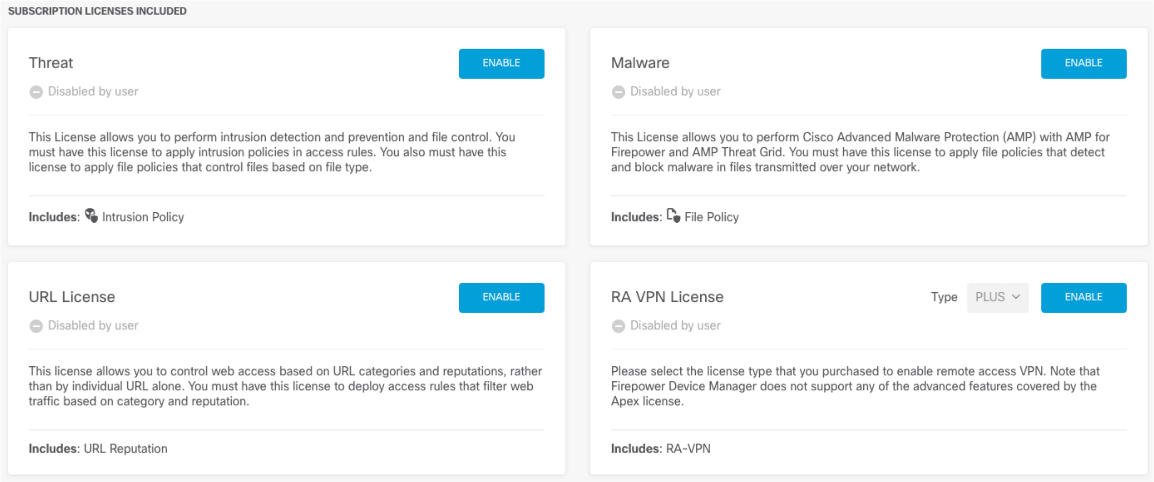
Device Summary

Smart License

✓ CONNECTED
SUFFICIENT LICENSE

Last sync: 10 Jul 2019 11:39 AM
Next sync: 10 Jul 2019 11:49 AM

Step 6 Click the **Enable/Disable** control for each optional license as desired.



SUBSCRIPTION LICENSES INCLUDED

Threat — ENABLE
Disabled by user

This License allows you to perform intrusion detection and prevention and file control. You must have this license to apply intrusion policies in access rules. You also must have this license to apply file policies that control files based on file type.

Includes: Intrusion Policy

Malware — ENABLE
Disabled by user

This License allows you to perform Cisco Advanced Malware Protection (AMP) with AMP for Firepower and AMP Threat Grid. You must have this license to apply file policies that detect and block malware in files transmitted over your network.

Includes: File Policy

URL License — ENABLE
Disabled by user

This license allows you to control web access based on URL categories and reputations, rather than by individual URL alone. You must have this license to deploy access rules that filter web traffic based on category and reputation.

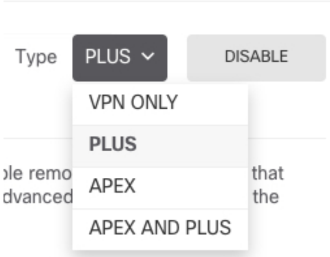
Includes: URL Reputation

RA VPN License — Type PLUS — ENABLE
Disabled by user

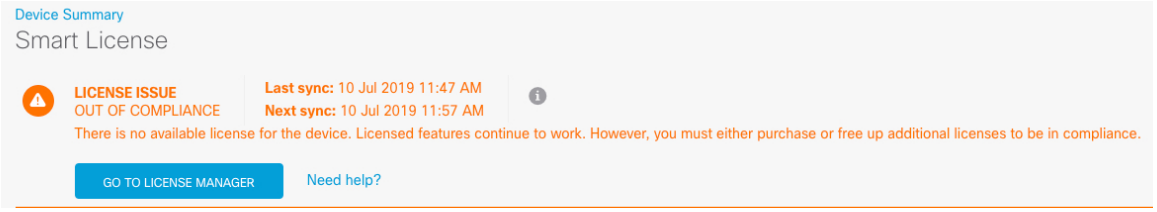
Please select the license type that you purchased to enable remote access VPN. Note that Firepower Device Manager does not support any of the advanced features covered by the Apex license.

Includes: RA-VPN

- **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:



Device Summary
Smart License

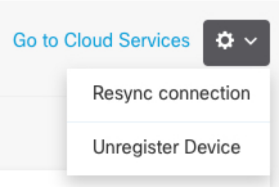
LICENSE ISSUE
OUT OF COMPLIANCE

Last sync: 10 Jul 2019 11:47 AM
Next sync: 10 Jul 2019 11:57 AM

There is no available license for the device. Licensed features continue to work. However, you must either purchase or free up additional licenses to be in compliance.

GO TO LICENSE MANAGER   Need help?

Step 7 Choose **Resync Connection** from the gear drop-down list to synchronize license information with Cisco Smart Software Manager.



Configure the Firewall in Firepower Device Manager

The following steps provide an overview of additional features you might want to configure. Please click the help button (**?**) on a page to get detailed information about each step.

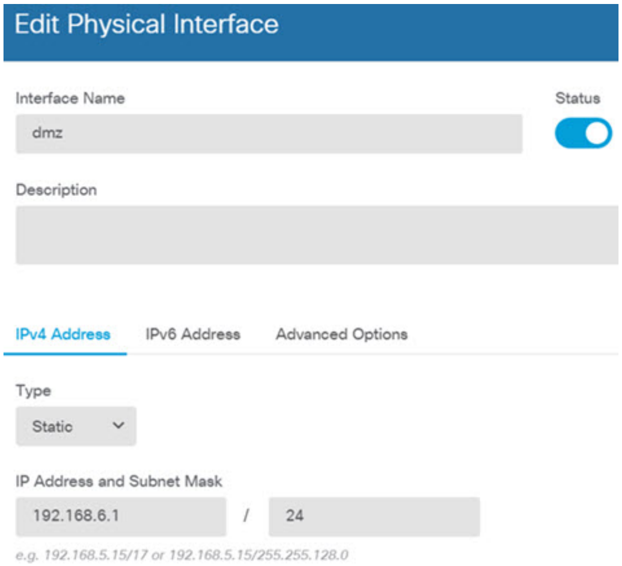
Procedure

Step 1 If you wired other interfaces, choose **Device**, and then click the link in the **Interfaces** summary.

Click the edit icon (✎) for each interface to set the mode and define the IP address and other settings.

The following example configures an interface to be used as a “demilitarized zone” (DMZ), where you place publicly-accessible assets such as your web server. Click **Save** when you are finished.

Figure 7: Edit Interface



Edit Physical Interface

Interface Name: dmz

Status: on

Description:

Type: Static

IP Address and Subnet Mask: 192.168.6.1 / 24

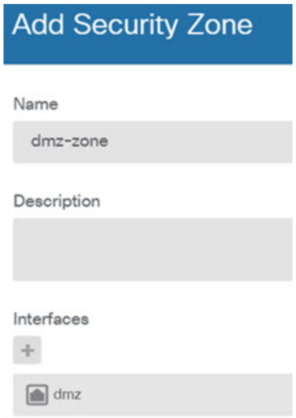
e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

Step 2 If you configured new interfaces, choose **Objects**, then select **Security Zones** from the table of contents.

Edit or create new zones as appropriate. Each interface must belong to a zone, because you configure policies based on security zones, not interfaces. You cannot put the interfaces in zones when configuring them, so you must always edit the zone objects after creating new interfaces or changing the purpose of existing interfaces.

The following example shows how to create a new dmz-zone for the dmz interface.

Figure 8: Security Zone Object



Add Security Zone

Name: dmz-zone

Description:

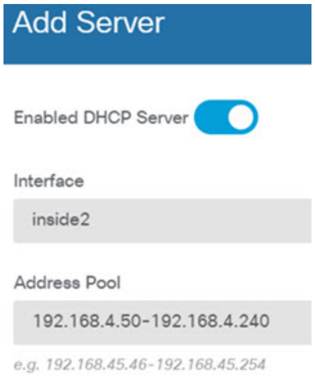
Interfaces

Step 3 If you want internal clients to use DHCP to obtain an IP address from the device, choose **Device** > **System Settings** > **DHCP Server**, then select the **DHCP Servers** tab.

There is already a DHCP server configured for the inside interface, but you can edit the address pool or even delete it. If you configured other inside interfaces, it is very typical to set up a DHCP server on those interfaces. Click + to configure the server and address pool for each inside interface.

You can also fine-tune the WINS and DNS list supplied to clients on the **Configuration** tab. The following example shows how to set up a DHCP server on the inside2 interface with the address pool 192.168.4.50-192.168.4.240.

Figure 9: DHCP Server



Add Server

Enabled DHCP Server: On

Interface: inside2

Address Pool: 192.168.4.50-192.168.4.240

e.g. 192.168.45.46-192.168.45.254

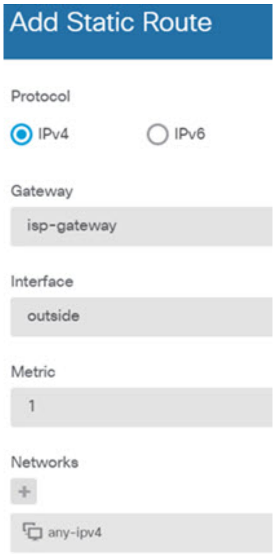
Step 4 Choose **Device**, then click **View Configuration** (or **Create First Static Route**) in the **Routing** group and configure a default route.

The default route normally points to the upstream or ISP router that resides off the outside interface. A default IPv4 route is for any-ipv4 (0.0.0.0/0), whereas a default IPv6 route is for any-ipv6 (::0/0). Create routes for each IP version you use. If you use DHCP to obtain an address for the outside interface, you might already have the default routes that you need.

Note The routes you define on this page are for the data interfaces only. They do not impact the management interface. Set the management gateway on **Device** > **System Settings** > **Management Interface**.

The following example shows a default route for IPv4. In this example, isp-gateway is a network object that identifies the IP address of the ISP gateway (you must obtain the address from your ISP). You can create this object by clicking **Create New Network** at the bottom of the **Gateway** drop-down list.

Figure 10: Default Route



Add Static Route

Protocol

● IPv4 ○ IPv6

Gateway: isp-gateway

Interface: outside

Metric: 1

Networks: any-ipv4

Step 5 Choose **Policies** and configure the security policies for the network.

The device setup wizard enables traffic flow between the inside-zone and outside-zone, and interface NAT for all interfaces when going to the outside interface. Even if you configure new interfaces, if you add them to the inside-zone object, the access control rule automatically applies to them.

However, if you have multiple inside interfaces, you need an access control rule to allow traffic flow from inside-zone to inside-zone. If you add other security zones, you need rules to allow traffic to and from those zones. These would be your minimum changes.

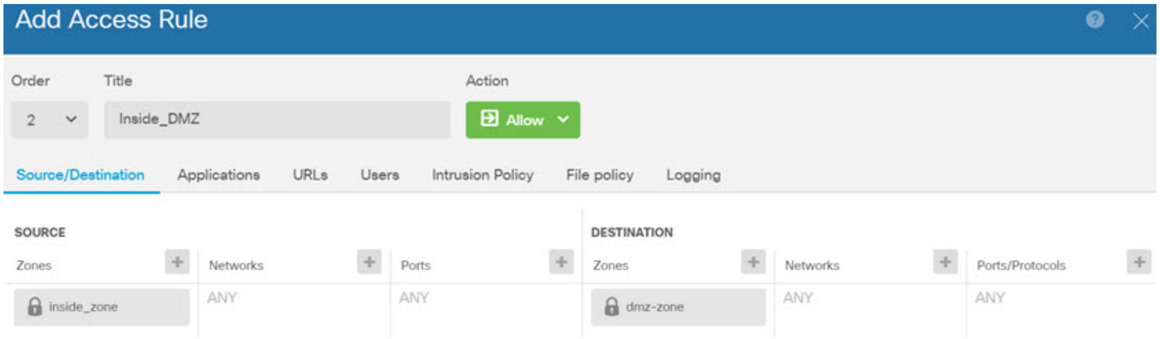
In addition, you can configure other policies to provide additional services, and fine-tune NAT and access rules to get the results that your organization requires. You can configure the following policies:

- **SSL Decryption**—If you want to inspect encrypted connections (such as HTTPS) for intrusions, malware, and so forth, you must decrypt the connections. Use the SSL decryption policy to determine which connections need to be decrypted. The system re-encrypts the connection after inspecting it.
- **Identity**—If you want to correlate network activity to individual users, or control network access based on user or user group membership, use the identity policy to determine the user associated with a given source IP address.
- **Security Intelligence**—Use the Security Intelligence policy to quickly drop connections from or to blacklisted IP addresses or URLs. By blacklisting known bad sites, you do not need to account for them in your access control policy. Cisco provides regularly updated feeds of known bad addresses and URLs so that the Security Intelligence blacklist updates dynamically. Using feeds, you do not need to edit the policy to add or remove items in the blacklist.
- **NAT (Network Address Translation)**—Use the NAT policy to convert internal IP addresses to externally routeable addresses.

- **Access Control**—Use the access control policy to determine which connections are allowed on the network. You can filter by security zone, IP address, protocol, port, application, URL, user or user group. You also apply intrusion and file (malware) policies using access control rules. Use this policy to implement URL filtering.
- **Intrusion**—Use the intrusion policies to inspect for known threats. Although you apply intrusion policies using access control rules, you can edit the intrusion policies to selectively enable or disable specific intrusion rules.

The following example shows how to allow traffic between the inside-zone and dmz-zone in the access control policy. In this example, no options are set on any of the other tabs except for **Logging**, where **At End of Connection** is selected.

Figure 11: Access Control Policy



Add Access Rule

Order: 2
Title: Inside_DMZ
Action: Allow

SOURCE

Zones	Networks	Ports
inside_zone	ANY	ANY

DESTINATION

Zones	Networks	Ports/Protocols
dmz-zone	ANY	ANY

Step 6 Choose **Device**, then click **View Configuration** in the **Updates** group and configure the update schedules for the system databases.

If you are using intrusion policies, set up regular updates for the Rules and VDB databases. If you use Security Intelligence feeds, set an update schedule for them. If you use geolocation in any security policies as matching criteria, set an update schedule for that database.

Step 7 Click the **Deploy** button in the menu, then click the Deploy Now button (), to deploy your changes to the device.

Changes are not active on the device until you deploy them.

Access the Firepower Threat Defense CLI

Use the command-line interface (CLI) to set up the system and do basic system troubleshooting. You cannot configure policies through a CLI session. You can access the CLI by connecting to the console port.

You can SSH to the management interface of the FTD device. You can also connect to the address on a data interface if you open the interface for SSH connections. SSH access to data interfaces is disabled by default.

Procedure

Step 1 To log into the CLI, connect your management computer to the console port.. The ASA 5508-X and 5516-X ship with a USB A-to-B serial cable. Be sure to install any necessary USB serial drivers for your operating system (see the hardware guide). Use the following serial settings:

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

Step 2 Log in to the FTD CLI using the **admin** username and the password you set at initial setup (the default is **Admin123**).

After logging in, for information on the commands available in the CLI, enter **help** or **?**. For usage information, see the *Cisco Firepower Threat Defense Command Reference*.

Power Off the Device

It's important that you shut down your system properly. Simply unplugging the power or pressing the power switch can cause serious file system damage. Remember that there are many processes running in the background all the time, and unplugging or shutting off the power does not allow the graceful shutdown of your Firepower system.

Procedure

Step 1 Connect to the console port to access the FTD CLI, and then shut down the FTD.

shutdown

Example:

```
> shutdown
This command will shutdown the system.  Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense......ok
Shutting down sfifd...                                                [  OK  ]
Clearing static routes
Unconfiguring default route                                           [  OK  ]
Unconfiguring address on br1                                          [  OK  ]
Unconfiguring IPv6                                                    [  OK  ]
Downing interface                                                     [  OK  ]
Stopping xinetd:
Stopping nscd...                                                      [  OK  ]
Stopping system log daemon...                                         [  OK  ]
Stopping Threat Defense ...
Stopping system message bus: dbus.                                    [  OK  ]
Un-mounting disk partitions ...
device-mapper: remove ioctl on root failed: Device or resource busy
```

```
[...]
mdadm: Cannot get exclusive access to /dev/md0:Perhaps a running process, mounted filesystem
 or active volume group?
Stopping OpenBSD Secure Shell server: sshd
stopped /usr/sbin/sshd (pid 3520)
done.
Stopping Advanced Configuration and Power Interface daemon: stopped /usr/sbin/acpid (pid
3525)
acpid.
Stopping system message bus: dbus.
Stopping internet superserver: xinetd.
no /etc/sysconfig/kdump.conf
Deconfiguring network interfaces... ifdown: interface br1 not configured
done.
SSP-Security-Module is shutting down ...
Sending ALL processes the TERM signal ...
acpid: exiting
Sending ALL processes the KILL signal ...
Deactivating swap...
Unmounting local filesystems...

Firepower Threat Defense stopped.
It is safe to power off now.

Do you want to reboot instead? [y/N]
```

Step 2 After the FTD shuts down, and the console shows that "It is safe to power off now", you can then turn off the power switch and unplug the power to physically remove power from the chassis if necessary.

Alternatively, you can reboot the system by typing **y** at the prompt.

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 FDM, see Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager.