Cisco Secure Firewall 3100 Getting Started Guide

First Published: 2022-02-24

Last Modified: 2024-09-04

Which Application and Manager is Right for You?

Your hardware platform can run one of two applications: Secure Firewall Threat Defense or ASA. For each application, you have a choice of managers. This chapter explains the application and manager choices.

Applications

You can use either of the following applications on your hardware platform:

- Threat Defense—The threat defense (formerly Firepower Threat Defense) is a next-generation firewall that combines an advanced stateful firewall, VPN concentrator, and next generation IPS.

- ASA—The ASA is a traditional, advanced stateful firewall and VPN concentrator.

Cisco provides ASA-to-threat defense migration tools to help you convert your ASA to the threat defense if you start with ASA and later reimage to threat defense.

To reimage between the ASA and the threat defense, see the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.

Managers

The threat defense and ASA support multiple managers.

Threat Defense Managers

Table 1: Threat Defense Managers

Manager	Description
Secure Firewall Management Center (formerly Firepower Management Center)	The management center is a multi-device manager that runs on its own server hardware, or as a virtual device on a hypervisor. For a local management center, see Threat Defense Deployment with the Management Center, on page 5. For a remote management center, see Threat Defense Deployment with a Remote Management Center, on page 47.
Cisco Defense Orchestrator (CDO) Cloud-delivered Firewall Management Center	CDO's cloud-delivered Firewall Management Center has all of the configuration functionality of an on-premises management center. For the analytics functionality, you can use a cloud solution or an on-prem management center. CDO also manages other security devices, such as ASAs. See Threat Defense Deployment with CDO, on page 123.
Secure Firewall Device Manager (formerly Firepower Device Manager)	The device manager is a simplified, on-device manager. Some threat defense features are not supported using the device manager. See Threat Defense Deployment with the Device Manager, on page 97.
Secure Firewall Threat Defense REST API	The threat defense REST API lets you automate direct configuration of the threat defense. You cannot use this API if you are managing the threat defense using the management center or CDO. The threat defense REST API is not covered in this guide. For more information, see the Cisco Secure Firewall Threat Defense REST API Guide.
Secure Firewall Management Center REST API	The management center REST API lets you automate configuration of management center policies that can then be applied to managed threat defenses. This API does not manage the threat defense directly. The management center REST API is not covered in this guide. For more information, see the Secure Firewall Management Center REST API Quick Start Guide.

ASA Managers

Table 2: ASA Managers

Manager	Description
CLI	You can use the CLI to configure all ASA functionality. The CLI is not covered in this guide. For more information, see the ASA configuration guides.

Manager	Description
Adaptive Security Device Manager (ASDM)	ASDM is a Java-based, on-device manager that provides full ASA functionality. See ASA Deployment with ASDM, on page 171.
CDO	CDO is a cloud-based, multi-device manager. CDO also manages other security devices, such as threat defenses. CDO for ASA is not covered in this guide. To get started with CDO, see the CDO home page.
Cisco Security Manager (CSM)	CSM is a multi-device manager that runs on its own server hardware. CSM does not support managing the threat defenses. CSM is not covered in this guide. For more information, see the CSM user guide.
ASA HTTP Interface	Using HTTP, an automation tool can execute commands on the ASAs by accessing specifically formatted URLs. The ASA HTTP interface is not covered in this guide. For more information, see the Cisco Secure Firewall ASA HTTP Interface for Automation.

Threat Defense Deployment with the Management Center

Is This Chapter for You?

To see all available applications and managers, see Which Application and Manager is Right for You?, on page 1. This chapter applies to the threat defense with the management center.

This chapter explains how to manage the threat defense with a management center located on your management network. For remote branch deployment, where the management center resides at a central headquarters, see Threat Defense Deployment with a Remote Management Center, on page 47.

About the Firewall

The hardware can run either threat defense software or ASA software. Switching between threat defense and ASA requires you to reimage the device. You should also reimage if you need a different software version than is currently installed. See Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.

The firewall runs an underlying operating system called the Secure Firewall eXtensible Operating System (FXOS). The firewall does not support the FXOS Secure Firewall chassis manager; only a limited CLI is supported for troubleshooting purposes. See the Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 and Secure Firewall 3100/4200 with Firepower Threat Defense for more information.

Privacy Collection Statement—The firewall 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.
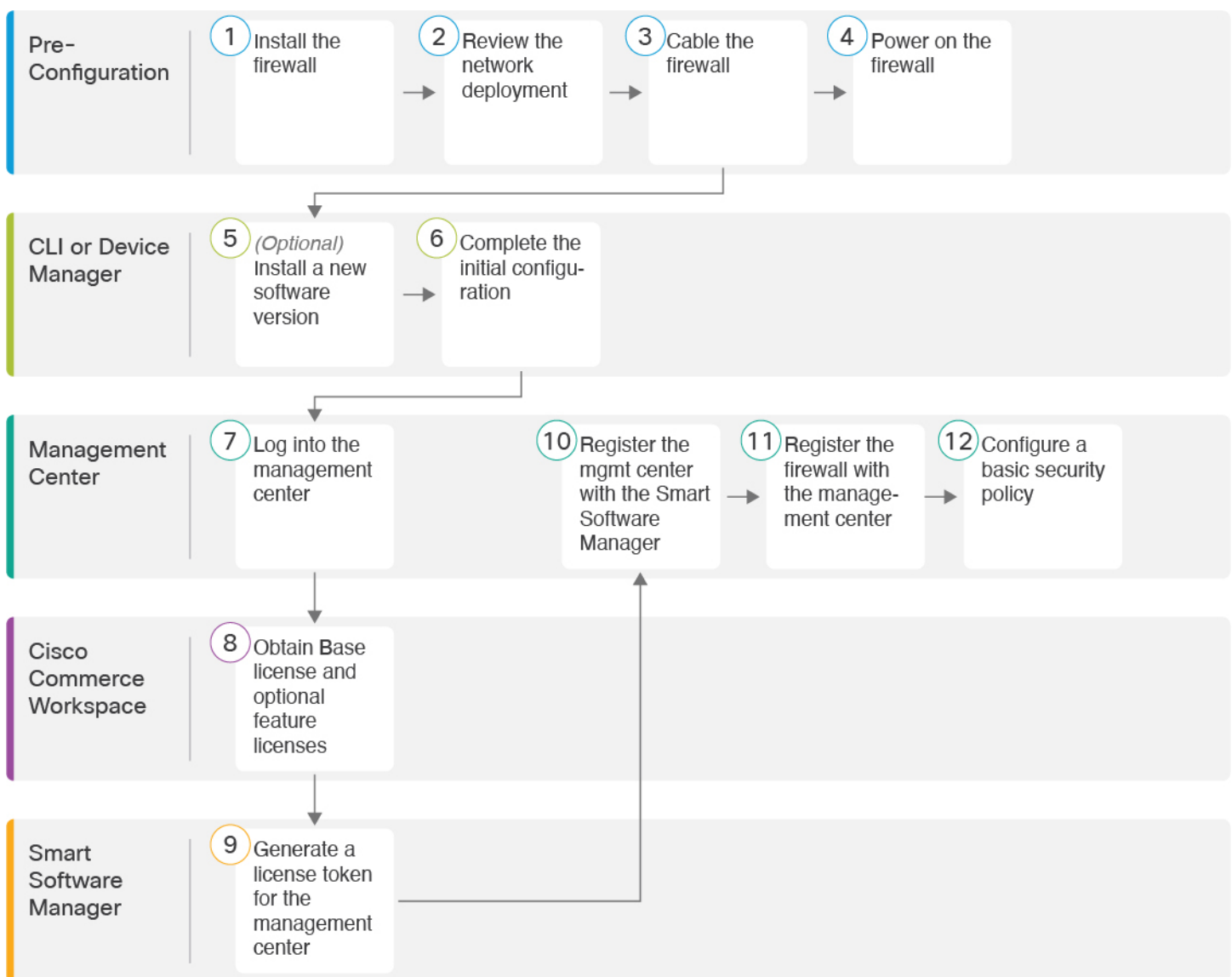
Before You Start

Deploy and perform initial configuration of the management center. See the getting started guide for your model.

End-to-End Tasks

| Pre-Configuration | ① Install the firewall | ② Review the network deployment | ③ Cable the firewall | ④ Power on the firewall |

| CLI or Device Manager | ⑤ *(Optional)* Install a new software version | ⑥ Complete the initial configuration |

| Management Center | ⑦ Log into the management center | ⑩ Register the mgmt center with the Smart Software Manager | ⑪ Register the firewall with the management center | ⑫ Configure a basic security policy |

| Cisco Commerce Workspace | ⑧ Obtain Base license and optional feature licenses |

| Smart Software Manager | ⑨ Generate a license token for the management center |

1	Pre-Configuration	Install the firewall. See the hardware installation guide.
2	Pre-Configuration	Review the Network Deployment, on page 7.
3	Pre-Configuration	Cable the Firewall, on page 9.
4	Pre-Configuration	Power on the Firewall, on page 11.
5	CLI	(Optional) Check the Software and Install a New Version, on page 12.
6	CLI or Device Manager	Complete the Threat Defense Initial Configuration, on page 14.
7	Management Center	Log Into the Management Center, on page 22.
8	Cisco Commerce Workspace	Buy Base license and optional feature licenses (Obtain Licenses for the Management Center, on page 22).
9	Smart Software Manager	Generate a license token for the management center (Obtain Licenses for the Management Center, on page 22).
10	Management Center	Register the management center with the Smart Licensing server (Obtain Licenses for the Management Center, on page 22).
11	Management Center	Register the Threat Defense with the Management Center, on page 24.
12	Management Center	Configure a Basic Security Policy, on page 28.

Review the Network Deployment

Management Interface

The management center communicates with the threat defense on the Management interface.

The dedicated Management interface is a special interface with its own network settings:

- By default, the Management 1/1 interface is enabled and configured as a DHCP client. If your network does not include a DHCP server, you can set the Management interface to use a static IP address during initial setup at the console port.

- Both the threat defense and the management center require internet access from their management interfaces for licensing and updates.

✎

Note	The management connection is a secure, TLS-1.3-encrypted communication channel between itself and the device. You do not need to run this traffic over an additional encrypted tunnel such as Site-to-Site VPN for security purposes. If the VPN goes down, for example, you will lose your management connection, so we recommend a simple management path.

### Data Interfaces

You can configure other interfaces after you connect the threat defense to the management center.

Typical Separate Management Network Deployment

The following figure shows a typical network deployment for the firewall where the threat defense, management center, and management computer connect to the management network.

The management network has a path to the internet for licensing and updates.

Figure 1: Separate Management Network
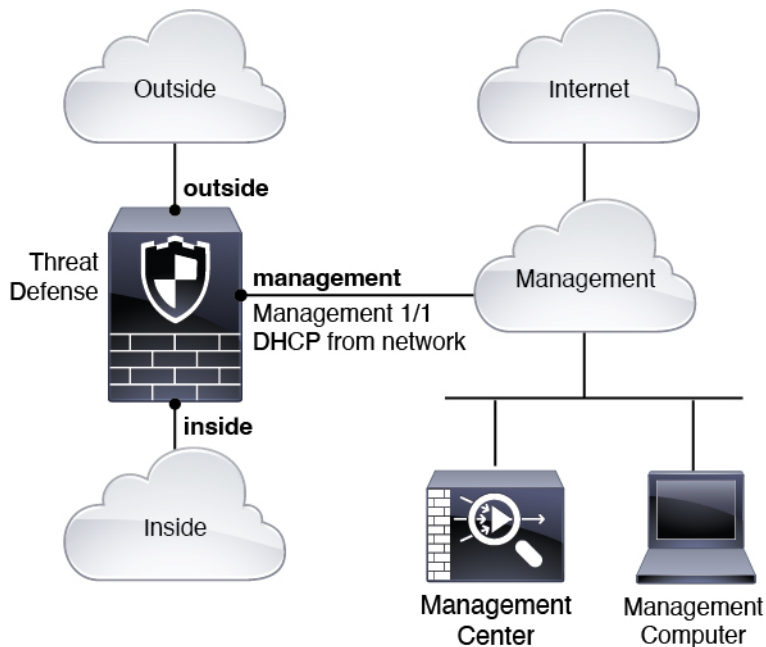
Typical Edge Network Deployment

The following figure shows a typical network deployment for the firewall where:

- Inside acts as the internet gateway for Management and for the management center.
- Management 1/1 connects to an inside interface through a Layer 2 switch.
- The management center and management computer connect to the switch.

This direct connection is allowed because the Management interface has separate routing from the other interfaces on the threat defense.

Figure 2: Edge Network Deployment
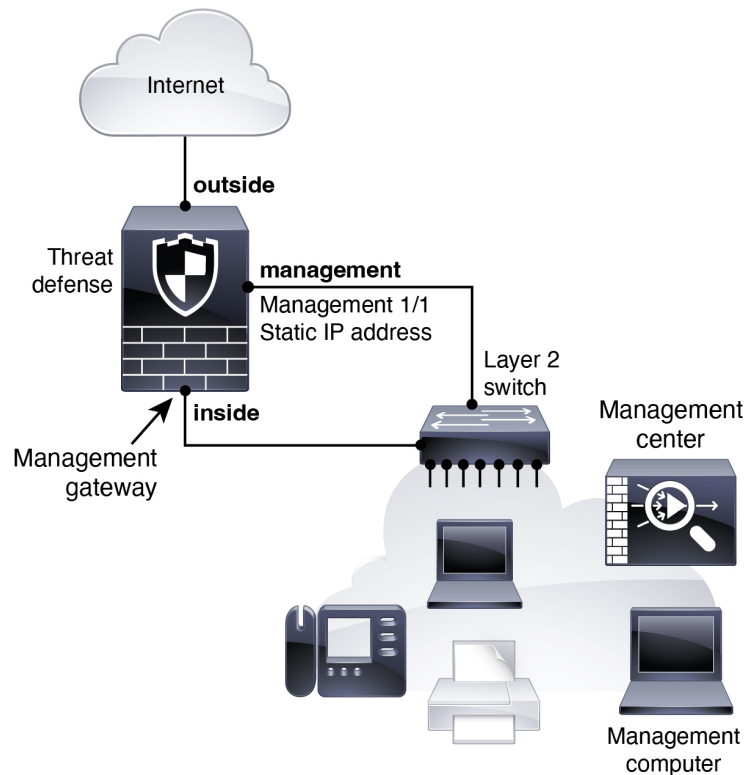
Cable the Firewall

To cable one of the recommended scenarios on the Secure Firewall 3100, see the following steps.

Note   Other topologies can be used, and your deployment will vary depending on your basic logical network connectivity, ports, addressing, and configuration requirements.

Before you begin

- Install an SFP for the Management port—The Management port is a 1/10-Gb SFP port that requires an SFP module.

- Obtain a console adapter—The Secure Firewall 3100 ships with a DB-9 to RJ-45 serial cable, so you may need to buy a third party DB-9-to-USB serial cable to make the connection.

Procedure

**Step 1**   Install the chassis. See the hardware installation guide.

Step 2   Cable for a separate management network:
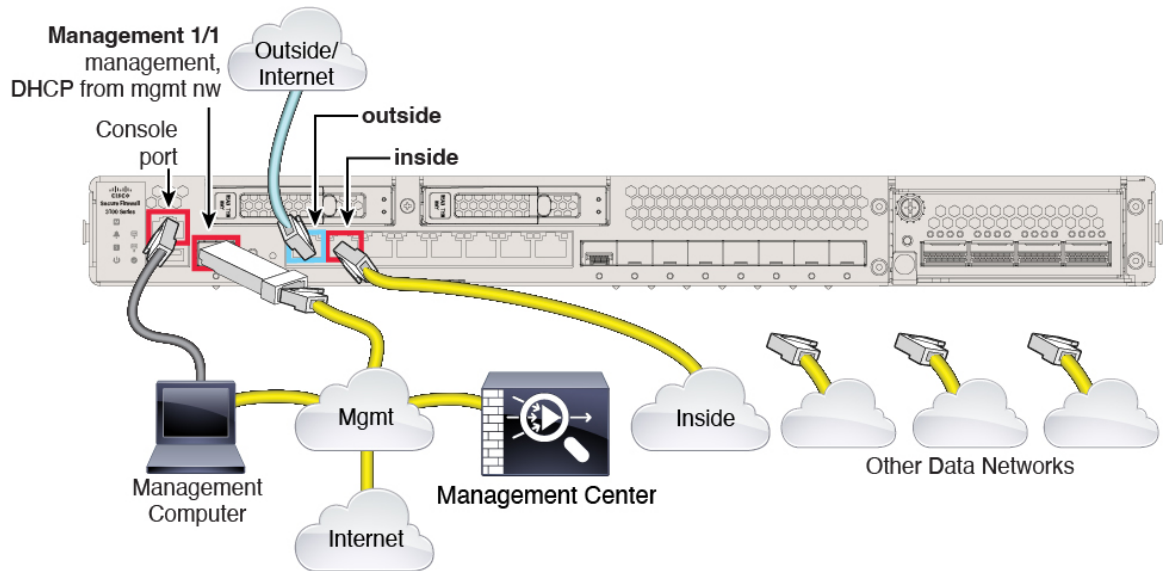
a) Cable the following to your management network:

- Management 1/1 interface

- Secure Firewall Management Center

- Management computer

b) Connect the management computer to the console port. You need to use the console port to access the CLI for initial setup if you do not use SSH to the Management interface.

c) Connect the inside interface (for example, Ethernet 1/2) to your inside router.

d) Connect the outside interface (for example, Ethernet 1/1) to your outside router.

e) Connect other networks to the remaining interfaces.

Step 3 Cable for an edge deployment:

Figure 4: Cabling an Edge Deployment
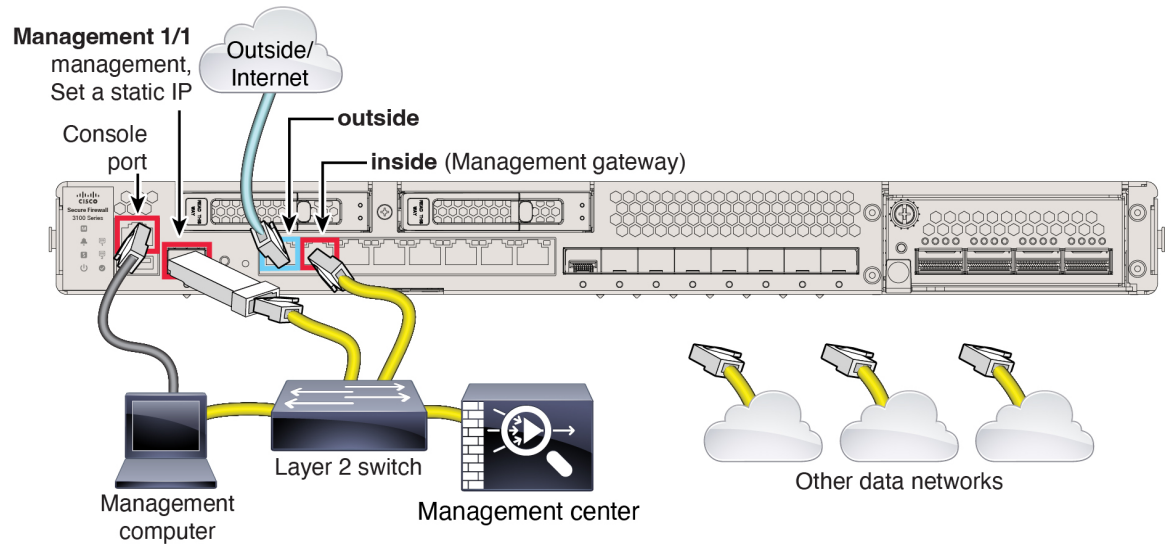
a) Cable the following to a Layer 2 Ethernet switch:

   • Inside interface (for example, Ethernet 1/2)

   • Management 1/1 interface

   • Secure Firewall Management Center

   • Management computer

b) Connect the management computer to the console port. You need to use the console port to access the CLI for initial setup.

c) Connect the outside interface (for example, Ethernet 1/1) to your outside router.

d) Connect other networks to the remaining interfaces.

Power on the Firewall

System power is controlled by a rocker power switch located on the rear of the firewall. The power switch is implemented as a soft notification switch that supports graceful shutdown of the system to reduce the risk of system software and data corruption.

Note   The first time you boot up the threat defense, initialization can take approximately 15 to 30 minutes.
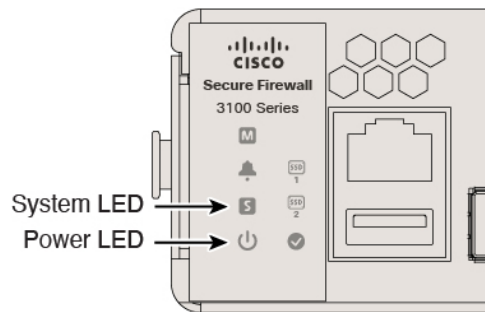
Before you begin

It's important that you provide reliable power for your firewall (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 firewall, 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 back of the firewall; if it is solid green, the firewall is powered on.

Figure 5: System and Power LEDs

Step 4 Check the System LED on the back of the firewall; after it is solid green, the system has passed power-on diagnostics.

Note When the switch is toggled from ON to OFF, it may take several seconds for the system to eventually power off. During this time, the Power LED on the front of the chassis blinks green. Do not remove the power until the Power LED is completely off.

(Optional) Check the Software and Install a New Version

To check the software version and, if necessary, install a different version, perform these steps. We recommend that you install your target version before you configure the firewall. Alternatively, you can perform an upgrade after you are up and running, but upgrading, which preserves your configuration, may take longer than using this procedure.

What Version Should I Run?

Cisco recommends running a Gold Star release indicated by a gold star next to the release number on the software download page. You can also refer to the release strategy described in https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html; for example, this bulletin describes short-term release numbering (with the latest features), long-term release numbering (maintenance releases and patches for a longer period of time), or extra long-term release numbering (maintenance releases and patches for the longest period of time, for government certification).

Procedure

Step 1 Connect to the console port. See Access the Threat Defense and FXOS CLI, on page 43 for more information.

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

You connect to the FXOS CLI. The first time you log in, you are prompted to change the password. This password is also used for the threat defense login for SSH.

Note If the password was already changed, and you do not know it, you must perform a factory reset to reset the password to the default. See the FXOS troubleshooting guide for the factory reset procedure.

Example:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Step 2 At the FXOS CLI, show the running version.

scope ssa

show app-instance

Example:

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name    Slot ID    Admin State    Operational State    Running Version Startup
 Version Cluster Oper State
-------------------- ---------- -------------- -------------------- ---------------
-------------- -----------------
ftd                 1          Enabled        Online               7.6.0.65        7.6.0.65
        Not Applicable
```

Step 3 If you want to install a new version, perform these steps.

a) If you need to set a static IP address for the Management interface, see Complete the Threat Defense Initial Configuration Using the CLI, on page 14. By default, the Management interface uses DHCP.

You will need to download the new image from a server accessible from the Management interface.

b) Perform the reimage procedure in the FXOS troubleshooting guide.

After the firewall reboots, you connect to the FXOS CLI again.

c) At the FXOS CLI, you are prompted to set the admin password again.

Complete the Threat Defense Initial Configuration

You can complete the threat defense initial configuration using the CLI or device manager.

Complete the Threat Defense Initial Configuration Using the CLI

Set the Management IP address, gateway, and other basic networking settings using the setup wizard. The dedicated Management interface is a special interface with its own network settings. If you do not want to use the Management interface for the manager access, you can use the CLI to configure a data interface instead. You will also configure the management center communication settings. When you perform initial setup using the device manager, *all* interface configuration completed in the device manager is retained when you switch to the management center for management, in addition to the Management interface and manager access interface settings. Note that other default configuration settings, such as the access control policy, are not retained.

Procedure

Step 1   Connect to the threat defense CLI, either from the console port or using SSH to the Management interface, which obtains an IP address from a DHCP server by default. If you intend to change the network settings, we recommend using the console port so you do not get disconnected.

The console port connects to the FXOS CLI. The SSH session connects directly to the threat defense CLI.

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

At the console port, you connect to the FXOS CLI. The first time you log in to FXOS, you are prompted to change the password. This password is also used for the threat defense login for SSH.

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 FXOS troubleshooting guide for the reimage procedure.

Example:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Step 3   If you connected to FXOS on the console port, connect to the threat defense CLI.

connect ftd

Example:

```
firepower# connect ftd
>
```

Step 4   The first time you log in to the threat defense, you are prompted to accept the End User License Agreement (EULA) and, if using an SSH connection, to change the admin password. You are then presented with the CLI setup script.

Note   You cannot repeat the CLI setup wizard 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 Cisco Secure Firewall Threat Defense Command Reference.

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

See the following guidelines:

- **Do you want to configure IPv4?** and/or **Do you want to configure IPv6?**—Enter **y** for at least one of these types of addresses. For the edge deployment example shown in the network deployment section, set a static IP address because the gateway inside interface does not yet have a DHCP server running.

- **Enter the IPv4 default gateway for the management interface** and/or **Enter the IPv6 gateway for the management interface**—Set a gateway IP address for Management 1/1 on the management network. In the edge deployment example shown in the network deployment section, the inside interface acts as the management gateway. In this case, you should set the gateway IP address to be the *intended* inside interface IP address; you must later use the management center to set the inside IP address. The **data-interfaces** setting applies only to the remote management center or device manager management.

- **If your networking information has changed, you will need to reconnect**—If you are connected with SSH 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 **no** to use the management center. A **yes** answer means you will use the device manager instead.

- **Configure firewall mode?**—We recommend that you set the firewall mode at initial configuration. Changing the firewall mode after initial setup erases your running configuration.

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.
Configure at least one of IPv4 or IPv6 unless managing via data interfaces.
Do you want to configure IPv4? (y/n) [y]:
```

```
          Do you want to configure IPv6? (y/n) [y]: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'
          [208.67.222.222,208.67.220.220,2620:119:35::35]:
          Enter a comma-separated list of search domains or 'none' []:cisco.com
          If your networking information has changed, you will need to reconnect.
          Disabling IPv6 configuration: management0
          Setting DNS servers: 208.67.222.222,208.67.220.220,2620:119:35::35
          Setting DNS domains:cisco.com
          Setting hostname as ftd-1.cisco.com
          Setting static IPv4: 10.10.10.15 netmask: 255.255.255.192 gateway: 10.10.10.1 on management0
          Updating routing tables, please wait...
          All configurations applied to the system. Took 3 Seconds.
          Saving a copy of running network configuration to local disk.
          For HTTP Proxy configuration, run 'configure network http-proxy'

          Manage the device locally? (yes/no) [yes]: no
          DHCP server is already disabled
          DHCP Server Disabled
          Configure firewall mode? (routed/transparent) [routed]:
          Configuring firewall mode ...

          Device is in OffBox mode - disabling/removing port 443 from iptables.
          Update policy deployment information
              - add device configuration
              - add network discovery
              - add system policy

          You can register the sensor to a Firepower Management Center and use the
          Firepower Management Center to manage it. Note that registering the sensor
          to a Firepower Management Center disables on-sensor Firepower Services
          management capabilities.

          When registering the sensor to a Firepower Management Center, a unique
          alphanumeric registration key is always required.  In most cases, to register
          a sensor to a Firepower Management Center, you must provide the hostname or
          the IP address along with the registration key.
          'configure manager add [hostname | ip address ] [registration key ]'

          However, if the sensor and the Firepower Management Center are separated by a
          NAT device, you must enter a unique NAT ID, along with the unique registration
          key.
          'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

          Later, using the web interface on the Firepower Management Center, you must
          use the same registration key and, if necessary, the same NAT ID when you add
          this sensor to the Firepower Management Center.
          >
```

Step 5 Identify the management center that will manage this threat defense.

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *reg_key* [*nat_id*]

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**}—Specifies either the FQDN or IP address of the management center. If the management center is not directly addressable, use **DONTRESOLVE** and also specify the *nat_id*. At least one of the devices, either the management center or the threat defense, must have a reachable IP address to establish the two-way, SSL-encrypted communication channel

between the two devices. If you specify **DONTRESOLVE** in this command, then the threat defense must have a reachable IP address or hostname.

- *reg_key*—Specifies a one-time registration key of your choice that you will also specify on the management center when you register the threat defense. The registration key must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-).

- *nat_id*—Specifies a unique, one-time string of your choice that you will also specify on the management center when you register the threat defense when one side does not specify a reachable IP address or hostname. It is required if you set the management center to **DONTRESOLVE**. The NAT ID must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID cannot be used for any other devices registering to the management center.

Example:

```
> configure manager add MC.example.com 123456
Manager successfully configured.
```

If the management center is behind a NAT device, enter a unique NAT ID along with the registration key, and specify DONTRESOLVE instead of the hostname, for example:

Example:

```
> configure manager add DONTRESOLVE regk3y78 natid90
Manager successfully configured.
```

If the threat defense is behind a NAT device, enter a unique NAT ID along with the management center IP address or hostname, for example:

Example:

```
> configure manager add 10.70.45.5 regk3y78 natid56
Manager successfully configured.
```

What to do next

Register your firewall to the management center.

Complete the Threat Defense Initial Configuration Using the Device Manager

When you use the device manager for initial setup, the following interfaces are preconfigured in addition to the Management interface and manager access settings. Note that other settings, such as the DHCP server on inside, access control policy, or security zones, are not configured.

- Ethernet 1/1—"outside", IP address from DHCP, IPv6 autoconfiguration

- Ethernet 1/2— "inside", 192.168.95.1/24

- Default route—Obtained through DHCP on the outside interface

If you perform additional interface-specific configuration within device manager before registering with the management center, then that configuration is preserved.

When you use the CLI, only the Management interface and manager access settings are retained (for example, the default inside interface configuration is not retained).

Procedure

Step 1 Log in to the device manager.

a) Enter one of the following URLs in your browser.

- Inside (Ethernet 1/2)—**https://192.168.95.1**.

- Management—**https://***management_ip*. The Management interface is a DHCP client, so the IP address depends on your DHCP server. You might have to set the Management IP address to a static address as part of this procedure, so we recommend that you use the inside interface so you do not become disconnected.

b) Log in with the username **admin**, and the default password **Admin123**.

c) You are prompted to read and accept the General Terms and change the admin password.

Step 2 Use the setup wizard when you first log into the device manager to complete the initial configuration. You can optionally skip the setup wizard by clicking **Skip device setup** at the bottom of the page.

After you complete the setup wizard, in addition to the default configuraton for the inside interface (Ethernet1/2), you will have configuration for an outside (Ethernet1/1) interface that will be maintained when you switch to management center management.

a) Configure the following options for the outside and management interfaces and click **Next**.

1. Outside Interface Address—This interface is typically the internet gateway, and might be used as your manager access interface. You cannot select an alternative outside interface during initial device setup. The first data interface is the default outside interface.

If you want to use a different interface from outside (or inside) for manager access, you will have to configure it manually after completing the setup wizard.

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.

2. Management Interface

You will not see Management Interface settings if you performed intial setup at the CLI. Note that setting the Management interface IP address is not part of the setup wizard. See Step to set the Management IP address.

DNS Servers—The DNS server for the firewall's Management interface. 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 firewall's Management interface.

b) Configure the **Time Setting (NTP)** and click **Next**.

1. **Time Zone**—Select the time zone for the system.

2. **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.

c) Select **Start 90 day evaluation period without registration**.

Do not register the threat defense with the Smart Software Manager; all licensing is performed on the management center.

d) Click **Finish**.

e) You are prompted to choose **Cloud Management** or **Standalone**. For management center management, choose **Standalone**, and then **Got It**.

Step 3 (Might be required) Configure a static IP address for the Management interface. See the Management interface on **Device** > **Interfaces**.

If you want to configure a static IP address, for example for an edge deployment where there is not DHCP server on the network yet, be sure to also set the default gateway to be a unique gateway instead of the data interfaces. If you use DHCP, you do not need to configure anything.

Step 4 If you want to configure additional interfaces, including an interface other than outside or inside, choose **Device**, and then click the link in the **Interfaces** summary.

See Configure the Firewall in the Device Manager, on page 115 for more information about configuring interfaces in the device manager. Other device manager configuration will not be retained when you register the device to the management center.

Step 5 Choose **Device** > **System Settings** > **Central Management**, and click **Proceed** to set up the management center management.

Step 6 Configure the **Management Center/CDO Details**.

Figure 6: Management Center/CDO Details

Configure Connection to Management Center or CDO

Provide details to register to the management center/CDO.

Management Center/CDO Details

Do you know the Management Center/CDO hostname or IP address?

◉ Yes   ○ No

Threat Defense   **Management Center/CDO**

10.89.5.16   10.89.5.35
fe80::6a87:c6ff:fea6:4c00/64

Management Center/CDO Hostname or IP Address

10.89.5.35

Management Center/CDO Registration Key

●●●●   👁

NAT ID

Required when the management center/CDO hostname or IP address is not provided. We recommend always setting the NAT ID even when you specify the management center/CDO hostname or IP address.

11203

Connectivity Configuration

Threat Defense Hostname

1120-3

DNS Server Group

CustomDNSServerGroup   ⌄

Management Center/CDO Access Interface

○ Data Interface

Please select an interface   ⌄

◉ Management Interface View details

CANCEL   CONNECT

a) For **Do you know the Management Center/**CDO **hostname or IP address**, click **Yes** if you can reach the management center using an IP address or hostname, or **No** if the management center is behind NAT or does not have a public IP address or hostname.

At least one of the devices, either the management center or the threat defense device, must have a reachable IP address to establish the two-way, TLS-1.3-encrypted communication channel between the two devices.

b) If you chose **Yes**, then enter the **Management Center/**CDO **Hostname/IP Address**.

c) Specify the **Management Center/**CDO **Registration Key**.

This key is a one-time registration key of your choice that you will also specify on the management center when you register the threat defense device. The registration key must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID can be used for multiple devices registering to the management center.

d) Specify a **NAT ID**.

This ID is a unique, one-time string of your choice that you will also specify on the management center. This field is required if you only specify the IP address on one of the devices; but we recommend that you specify the NAT ID even if you know the IP addresses of both devices. The NAT ID must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID *cannot* be used for any other devices registering to the management center. The NAT ID is used in combination with the IP address to verify that the connection is coming from the correct device; only after authentication of the IP address/NAT ID will the registration key be checked.

Step 7 Configure the **Connectivity Configuration**.

a) Specify the **FTD Hostname**.

b) Specify the **DNS Server Group**.

Choose an existing group, or create a new one. The default DNS group is called **CiscoUmbrellaDNSServerGroup**, which includes the OpenDNS servers.

c) For the **Management Center/CDO Access Interface**, choose **management**.

Step 8 Click **Connect**. The **Registration Status** dialog box shows the current status of the switch to the management center. After the **Saving Management Center/**CDO **Registration Settings** step, go to the management center, and add the firewall.

If you want to cancel the switch to the management center, click **Cancel Registration**. Otherwise, do not close the device manager browser window until after the **Saving Management Center/**CDO **Registration Settings** step. If you do, the process will be paused, and will only resume when you reconnect to the device manager.

If you remain connected to the device manager after the **Saving Management Center/**CDO **Registration Settings** step, you will eventually see the **Successful Connection with Management Center or** CDO dialog box, after which you will be disconnected from the device manager.

Figure 7: Successful Connection
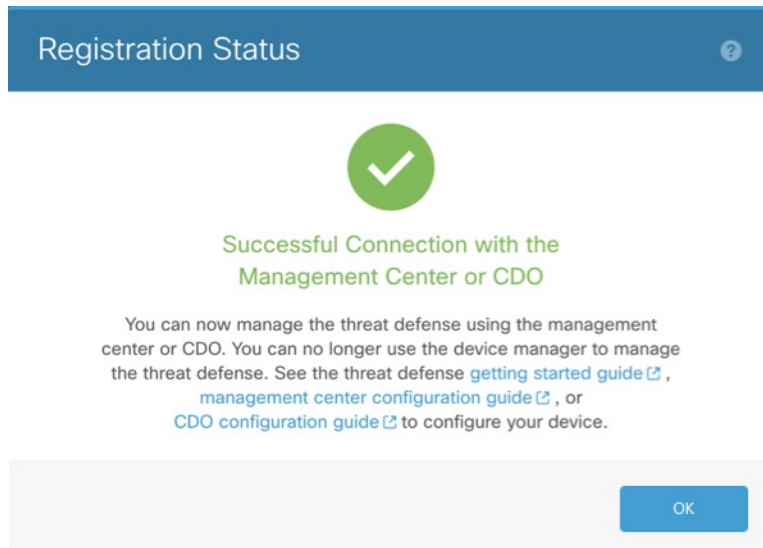
Log Into the Management Center

Use the management center to configure and monitor the threat defense.

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 Management Center

All licenses are supplied to the threat defense by the management center. You can purchase the following licenses:

- **Essentials**—(Required) Essentials license.

- **IPS**—Security Intelligence and Next-Generation IPS

- **Malware Defense**—Malware defense

- **URL Filtering**—URL Filtering

- **Cisco Secure Client**—Secure Client Advantage, Secure Client Premier, or Secure Client VPN Only

- **Carrier**—Diameter, GTP/GPRS, M3UA, SCTP

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

Before you begin

- Have an 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 an 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 **Search All** field on the Cisco Commerce Workspace.

Figure 8: License Search
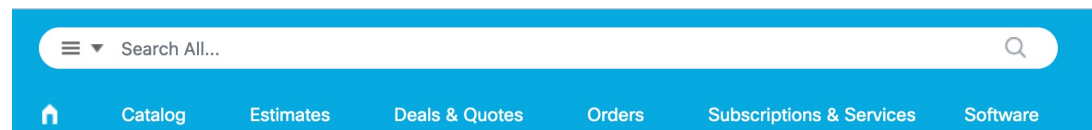
Choose **Products & Services** from the results.

Figure 9: Results

Search for the following license PIDs:

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

- Essentials:

    - *Included automatically*

- IPS, Malware Defense, and URL license combination:

• L-FPR3110T-TMC=

• L-FPR3120T-TMC=

• L-FPR3130T-TMC=

• L-FPR3140T-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-FPR3110T-TMC-1Y

• L-FPR3110T-TMC-3Y

• L-FPR3110T-TMC-5Y

• L-FPR3120T-TMC-1Y

• L-FPR3120T-TMC-3Y

• L-FPR3120T-TMC-5Y

• L-FPR3130T-TMC-1Y

• L-FPR3130T-TMC-3Y

• L-FPR3130T-TMC-5Y

• L-FPR3140T-TMC-1Y

• L-FPR3140T-TMC-3Y

• L-FPR3140T-TMC-5Y

• Carrier license:

• L-FPR3K-FTD-CAR=

• Cisco Secure Client—See the Cisco Secure Client Ordering Guide.

Step 2 If you have not already done so, register the management center with the Smart Licensing server.

Registering requires you to generate a registration token in the Smart Software Manager. See the Cisco Secure Firewall Management Center Administration Guide for detailed instructions.

Register the Threat Defense with the Management Center

Register the threat defense to the management center manually using the device IP address or hostname.

Before you begin

Procedure

Step 1 In the management center, choose **Devices** > **Device Management**.

Step 2 From the **Add** drop-down list, choose **Add Device**.

Figure 10: Add Device Using a Registration Key

Add Device   ⓘ

☐ CDO Managed Device

Host:†

    10.89.5.41

Display Name:

    3110-1

Registration Key:*

    ••••

Group:

    None   ⌄

Access Control Policy:*

    wfx_automationPolicy123   ⌄

Smart Licensing

Note: All virtual Firewall Threat Defense devices require a performance tier license.
Make sure your Smart Licensing account contains the available licenses you need.
It's important to choose the tier that matches the license you have in your account.
Click here for information about the Firewall Threat Defense performance-tiered licensing.
Until you choose a tier, your Firewall Threat Defense virtual defaults to the FTDv50 selection.

Performance Tier (only for Firewall Threat Defense virtual 7.0 and above):

    Select a recommended Tier   ⌄

☑ Carrier
☑ Malware Defense
☑ IPS
☑ URL

Advanced

Unique NAT ID:†

    31101

☑ Transfer Packets

                        Cancel   **Register**

Figure 11: Add Device

Set the following parameters:

- **Host**—Enter the IP address or hostname of the threat defense you want to add. You can leave this field blank if you specified both the management center IP address and a NAT ID in the threat defense initial configuration.

  Note In an HA environment, when both the management centers are behind a NAT, you can register the threat defense without a host IP or name in the primary management center. However, for registering the threat defense in a secondary management center, you must provide the IP address or hostname for the threat defense.

- **Display Name**—Enter the name for the threat defense as you want it to display in the management center.

- **Registration Key**—Enter the same registration key that you specified in the threat defense initial 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 .

Figure 12: New Policy

- **Smart Licensing**—Assign the Smart Licenses you need for the features you want to deploy. **Note:** You can apply the Secure Client remote access VPN license after you add the device, from the **System** > **Licenses** > **Smart Licenses** page.

- **Unique NAT ID**—Specify the NAT ID that you specified in the threat defense initial configuration.

- **Transfer Packets**—Allow the device to transfer packets to the management center. When events like IPS or Snort are triggered with this option enabled, the device sends event metadata information and packet data to the management center for inspection. If you disable it, only event information will be sent to the management center, 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 threat defense fails to register, check the following items:

- Ping—Access the threat defense CLI, and ping the management center 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 threat defense Management IP address, use the **configure network** {**ipv4** | **ipv6**} **manual** command.

- Registration key, NAT ID, and the management center 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 threat defense using the **configure manager add** command.

For more troubleshooting information, see https://cisco.com/go/fmc-reg-error.

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 28.
2	Configure the DHCP Server, on page 33.
3	Add the Default Route, on page 35.
4	Configure NAT, on page 37.
5	Allow Traffic from Inside to Outside, on page 40.
6	Deploy the Configuration, on page 42.

Configure Interfaces

When you use the device manager for initial setup, the following interfaces are preconfigured:

- Ethernet 1/1—"outside", IP address from DHCP, IPv6 autoconfiguration

- Ethernet 1/2— "inside", 192.168.95.1/24

       • Default route—Obtained through DHCP on the outside interface

If you performed additional interface-specific configuration within device manager before registering with the management center, then that configuration is preserved.

In any case, you need to perform additional interface configuration after you register the device. Enable the threat defense interfaces, assign them to security zones, and set the IP addresses. Also configure breakout 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** (✐) for the firewall.

Step 2   Click **Interfaces**.

Figure 13: Interfaces

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	
● Management0/0	management	Physical				Disabled	Global	🔍 ⤳
GigabitEthernet0/0		Physical				Disabled		✎
GigabitEthernet0/1		Physical				Disabled		✎
GigabitEthernet0/2		Physical				Disabled		✎
GigabitEthernet0/3		Physical				Disabled		✎
GigabitEthernet0/4		Physical				Disabled		✎
GigabitEthernet0/5		Physical				Disabled		✎
GigabitEthernet0/6		Physical				Disabled		✎
GigabitEthernet0/7		Physical				Disabled		✎

Step 3   To create breakout ports from a 40-Gb or larger interface, click the **Break** icon for the interface.

If you already used the full interface in your configuration, you will have to remove the configuration before you can proceed with the breakout.

Step 4   Click **Edit** (✐) for the interface that you want to use for *inside*.

The **General** tab appears.

Figure 14: General Tab

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**

Figure 15: IPv4 Tab

Edit Physical Interface

| General | IPv4 | IPv6 | Path Monitoring |

IP Type:

Use Static IP ▾

IP Address:

192.168.1.1/24

eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

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

Figure 16: IPv6 Tab

Edit Physical Interface

| General | IPv4 | IPv6 | Path Monitoring | Hardware Configu |

| Basic | Address | Prefixes | Settings | DHCP |

Enable IPV6: ☐

Enforce EUI 64: ☐

Link-Local address: _____

Autoconfiguration: ☑

Obtain Default Route: ☐

    f) Click **OK**.

Step 5 Click the **Edit** (✎) for the interface that you want to use for *outside*.

The **General** tab appears.

Figure 17: General Tab

Edit Physical Interface

| General | IPv4 | IPv6 | Path Monitoring | Hardwar |

Name:

outside

☑ Enabled

☐ Management Only

Description:

Mode:

None ▼

Security Zone:

outside_zone ▼

Interface ID:

GigabitEthernet0/0

MTU:

1500

(64 - 9000)

Priority:

0   *(0 - 65535)*

Propagate Security Group Tag: ☐

NVE Only:

☐

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.

Figure 18: IPv4 Tab

Edit Physical Interface

| General | IPv4 | IPv6 | Path Mo |

IP Type:

Use DHCP ▼

Obtain default route
using DHCP: ☑

DHCP route metric:

1

(1 – 255)

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

Figure 19: IPv6 Tab

Edit Physical Interface

| General | IPv4 | IPv6 | Path Monitoring | Hardware Configu |

| Basic | Address | Prefixes | Settings | DHCP |

Enable IPV6: ☐

Enforce EUI 64: ☐

Link-Local address:

Autoconfiguration: ☑

Obtain Default Route: ☐

    f) Click **OK**.

Step 6 Click **Save**.

Configure the DHCP Server

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

Procedure

Step 1 Choose **Devices** > **Device Management**, and click **Edit** (✎) for the device.

Step 2 Choose **DHCP** > **DHCP Server**.

Figure 20: DHCP Server

Step 3 On the **Server** page, click **Add**, and configure the following options:

Figure 21: Add Server

- **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 **Edit** (✐) for the device.

Step 2   Choose **Routing** > **Static Route**.

Figure 22: Static Route
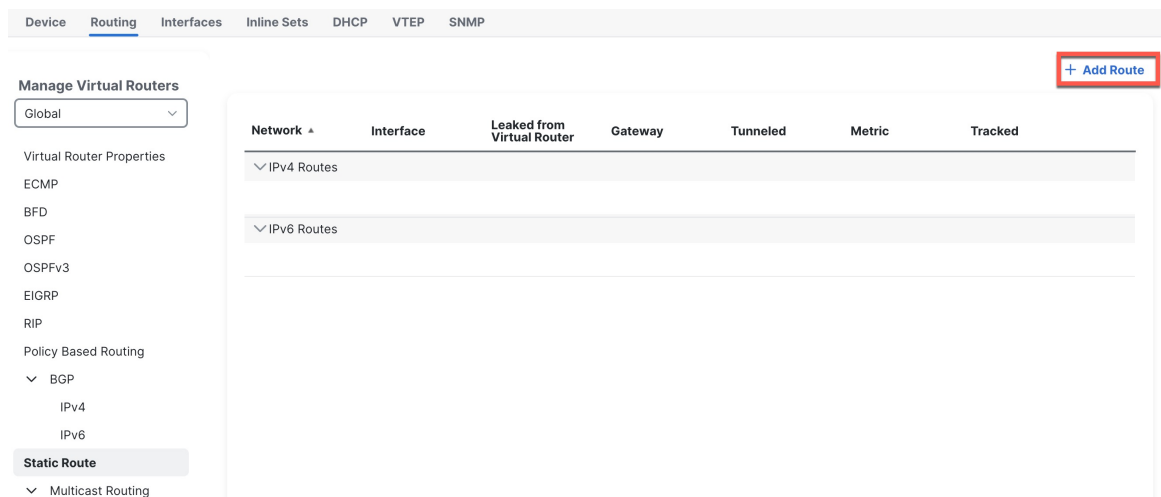
Step 3   Click **Add Route**, and set the following:

Figure 23: Add Static Route Configuration

- **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.

- **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 4   Click **OK**.

The route is added to the static route table.

Step 5   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**.

Figure 24: New Policy

The policy is added the management center. You still have to add rules to the policy.

Figure 25: NAT Policy

Step 3 Click **Add Rule**.

The **Add NAT Rule** dialog box appears.

Step 4 Configure the basic rule options:

Figure 26: 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.

Figure 27: Interface Objects

Step 6 On the **Translation** page, configure the following options:

Figure 28: Translation

Interface Objects	Translation	PAT Pool	Advanced

Original Packet

Original Source:*
all-ipv4 +

Original Port:
TCP

Translated Packet

Translated Source:
Destination Interface IP

ⓘ The values selected for Destination Interface Objects in 'Interface Objects' tab will be used

Translated Port:

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

Figure 29: New Network Object

New Network Object ⓘ

Name
all-ipv4

Description

Network
○ Host ○ Range ● Network ○ FQDN

0.0.0.0/0

☐ Allow Overrides

Cancel **Save**

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 threat defense, 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.

Procedure

Step 1 Choose **Policy** > **Access Policy** > **Access Policy**, and click **Edit** (✐) for the access control policy assigned to the threat defense.

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

Figure 30: Source Zone
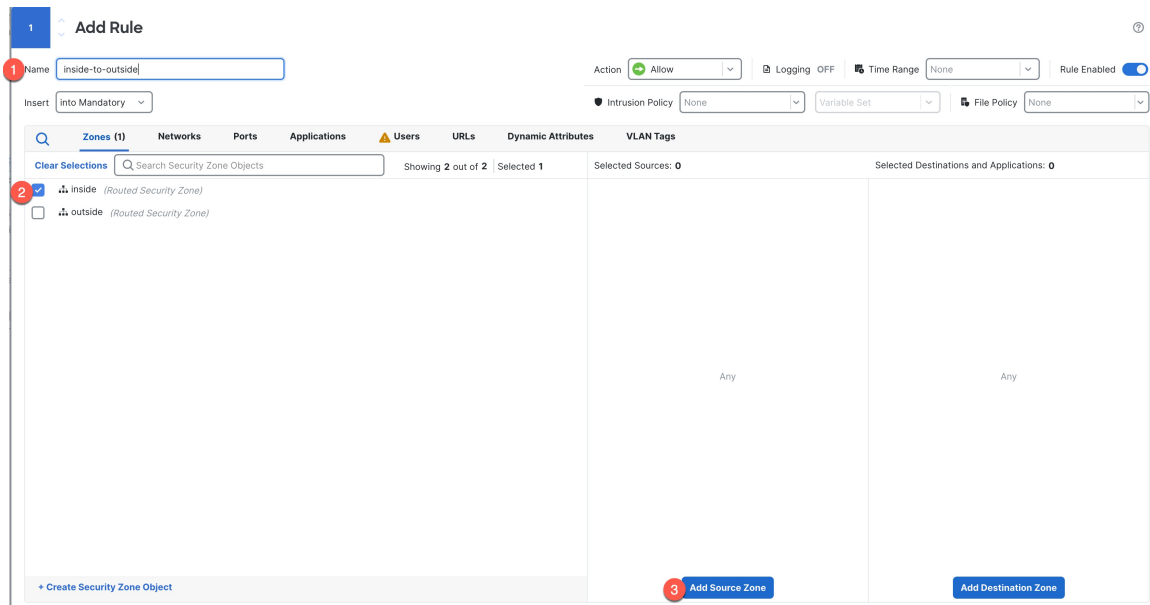
Figure 31: Destination Zone
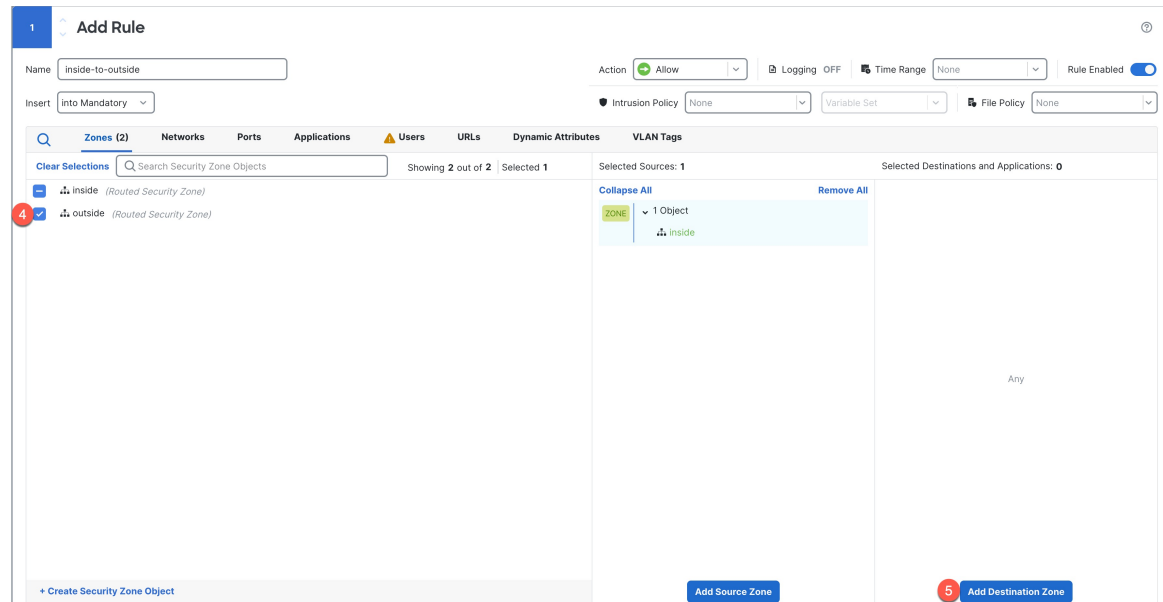
Figure 32: Apply
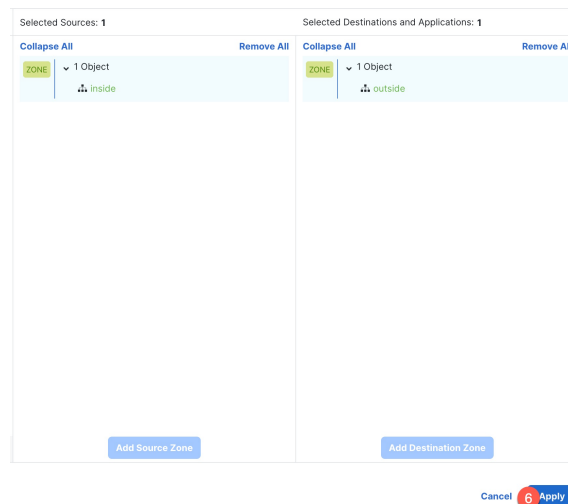
- **Name**—Name this rule, for example, **inside-to-outside**.

- **Selected Sources**—Select the inside zone from **Zones**, and click **Add Source Zone**.

- **Selected Destinations and Applications**—Select the outside zone from **Zones**, and click **Add Destination Zone**.

Leave the other settings as is.

Step 3 Click **Apply**.

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

Step 4   Click **Save**.

Deploy the Configuration

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

Procedure

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

Figure 33: Deploy
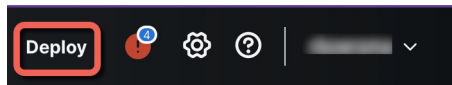
Step 2   For a quick deployment, check specific devices and then click **Deploy**, or click **Deploy All** to deploy to all devices. Otherwise, for additional deployment options, click **Advanced Deploy**.

Figure 34: Deploy Selected
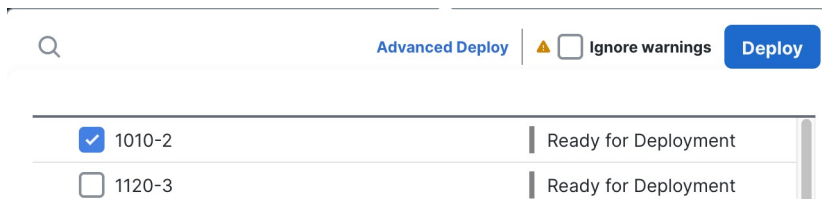
Figure 35: Deploy All
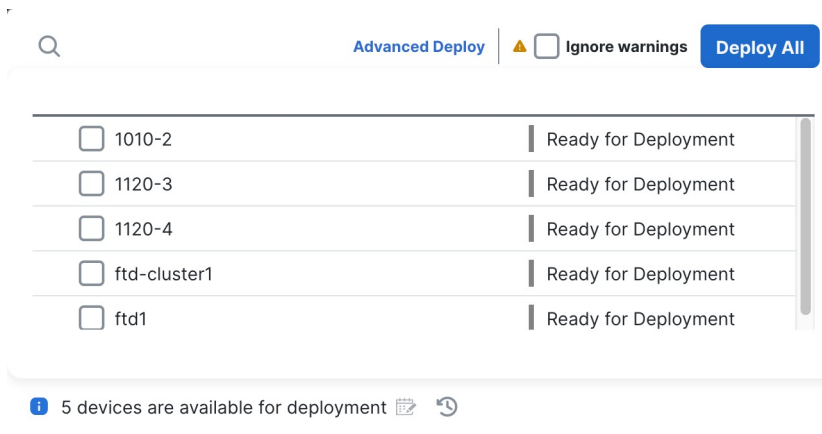
Figure 36: Advanced Deploy
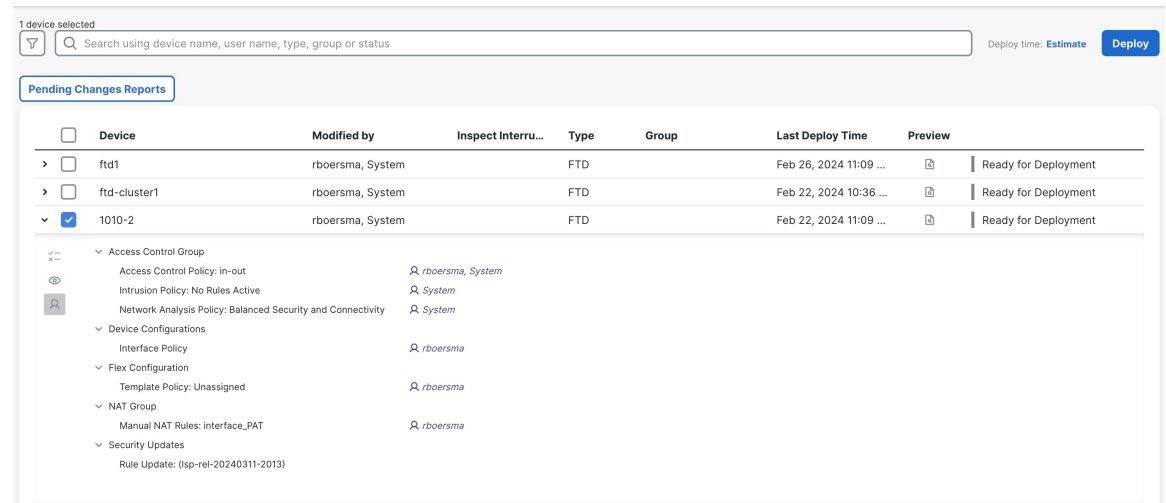
Step 3 Ensure that the deployment succeeds. Click the icon to the right of the **Deploy** button in the menu bar to see status for deployments.

Figure 37: Deployment Status

Access the Threat Defense and FXOS 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 also access the FXOS CLI for troubleshooting purposes.

Note   You can alternatively SSH to the Management interface of the threat defense device. Unlike a console session, the SSH session defaults to the threat defense CLI, from which you can connect to the FXOS CLI using the **connect fxos** command. You can later 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. This procedure describes console port access, which defaults to the FXOS CLI.

Procedure

Step 1   To log into the CLI, connect your management computer to the console port. The Secure Firewall 3100 ships with a DB-9 to RJ-45 serial cable, so you may need to buy a third party DB-9-to-USB serial cable to make the connection. Be sure to install any necessary USB serial drivers for your operating system. The console port defaults to the FXOS CLI. Use the following serial settings:

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

You connect to the FXOS CLI. Log in to the CLI using the **admin** username and the password you set at initial setup (the default is **Admin123**).

Example:

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

Step 2   Access the threat defense CLI.

connect ftd

Example:

```
firepower# connect ftd
>
```

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

Step 3   To exit the threat defense CLI, enter the **exit** or **logout** command.

This command returns you to the FXOS CLI prompt. For information on the commands available in the FXOS CLI, enter **?**.

Example:

```
> exit
firepower#
```

Power Off the Firewall

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 firewall system.

You can power off the device using the management center device management page, or you can use the FXOS CLI.

Power Off the Firewall Using the Management Center

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 firewall.

You can shut down your system properly using the management center.

Procedure

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the device that you want to restart, click **Edit** (✐).

Step 3 Click the **Device** tab.

Step 4 Click **Shut Down Device** (⊗) in the **System** section.

Step 5 When prompted, confirm that you want to shut down the device.

Step 6 If you have a console connection to the firewall, monitor the system prompts as the firewall shuts down. You will see the following prompt:

```
System is stopped.
It is safe to power off now.

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

If you do not have a console connection, wait approximately 3 minutes to ensure the system has shut down.

Step 7 You can now turn off the power switch and unplug the power to physically remove power from the chassis if necessary.

Power Off the Firewall at the CLI

You can use the FXOS CLI to safely shut down the system and power off the device. You access the CLI by connecting to the console port; see Access the Threat Defense and FXOS CLI, on page 43.

Procedure

Step 1 In the FXOS CLI, connect to local-mgmt:

firepower # **connect local-mgmt**

Step 2 Issue the **shutdown** command:

firepower(local-mgmt) # **shutdown**

Example:

```
firepower(local-mgmt)# shutdown
This command will shutdown the system.   Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense......ok
```

Step 3 Monitor the system prompts as the firewall shuts down. You will see the following prompt:

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

Step 4 You can now turn off the power switch and unplug the power to physically remove power from the chassis if necessary.

What's Next?

To continue configuring your threat defense, see the documents available for your software version at Navigating the Cisco Secure Firewall Threat Defense Documentation.

For information related to using the management center, see the Cisco Secure Firewall Management Center Device Configuration Guide.

Threat Defense Deployment with a Remote Management Center

Is This Chapter for You?

To see all available applications and managers, see Which Application and Manager is Right for You?, on page 1. This chapter applies to the threat defense with the management center.

This chapter explains how to manage the threat defense with a management center located at a central headquarters. For local deployment, where the management center resides on your local management network, see Threat Defense Deployment with the Management Center, on page 5.

About the Firewall

The hardware can run either threat defense software or ASA software. Switching between threat defense and ASA requires you to reimage the device. You should also reimage if you need a different software version than is currently installed. See Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.

The firewall runs an underlying operating system called the Secure Firewall eXtensible Operating System (FXOS). The firewall does not support the FXOS Secure Firewall chassis manager; only a limited CLI is supported for troubleshooting purposes. See the Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 and Secure Firewall 3100/4200 with Firepower Threat Defense for more information.

Privacy Collection Statement—The firewall 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.

How Remote Management Works

To allow the management center to manage the threat defense over the internet, use the outside interface for management center manager access instead of the Management interface. Because most remote branch offices only have a single internet connection, outside manager access makes centralized management possible.

Note The management connection is a secure, TLS-1.3-encrypted communication channel between itself and the device. You do not need to run this traffic over an additional encrypted tunnel such as Site-to-Site VPN for security purposes. If the VPN goes down, for example, you will lose your management connection, so we recommend a simple management path.

Registration Methods

Use one of the following methods to provision your threat defense:

Zero-Touch Provisioning (Management Center 7.4 and later, Threat Defense 7.2 and later)

1. Send the threat defense to the remote branch office. Do not configure anything on the device, because zero-touch provisioning may not work with pre-configured devices.

Note You can preregister the threat defense on the management center using the threat defense serial number before sending the device to the branch office. The management center integrates with the Cisco Security Cloud and CDO for this functionality.

2. At the branch office, cable and power on the threat defense.

3. Finish registering the threat defense using the management center.

Manual Provisioning

1. Pre-configure the threat defense at the CLI or using the device manager, and then send the threat defense to the remote branch office.

2. At the branch office, cable and power on the threat defense.

3. Finish registering the threat defense using the management center.

Threat Defense Manager Access Interface

This guide covers **outside** interface access because it is the most likely scenario for remote branch offices. Although manager access occurs on the outside interface, the dedicated Management interface is still relevant. The Management interface is a special interface configured separately from the threat defense data interfaces, and it has its own network settings.

- The Management interface network settings are still used even though you are enabling manager access on a data interface.

- All management traffic continues to be sourced from or destined to the Management interface.

- When you enable manager access on a data interface, the threat defense forwards incoming management traffic over the backplane to the Management interface.

- For outgoing management traffic, the Management interface forwards the traffic over the backplane to the data interface.

Manager Access Requirements

Manager access from a data interface has the following limitations:

- You can only enable manager access on a physical, data interface. You cannot use a subinterface or EtherChannel, nor can you create a subinterface on the manager access interface. You can also use the management center to enable manager access on a single secondary interface for redundancy.

- This interface cannot be management-only.

- Routed firewall mode only, using a routed interface.

- PPPoE is not supported. If your ISP requires PPPoE, you will have to put a router with PPPoE support between the threat defense and the WAN modem.

- The interface must be in the global VRF only.

- SSH is not enabled by default for data interfaces, so you will have to enable SSH later using the management center. Because the Management interface gateway will be changed to be the data interfaces, you also cannot SSH to the Management interface from a remote network unless you add a static route for the Management interface using the **configure network static-routes** command.

- Clustering is not supported. You must use the Management interface in this case.

- High availability is not supported. You must use the Management interface in this case.

Zero-Touch Provisioning Network

The following figure shows a typical network deployment for the firewall where:

- The management center is at central headquarters.

- The threat defense uses the outside interface for manager access.

- Either the threat defense or management center needs a public IP address or hostname to allow the inbound management connection, although you do not need to know the IP address for registration. For pre-7.2(4) and 7.3 threat defense versions, the management center needs to be publicly reachable.

- Both the management center and threat defense initially communicate with the Cisco Security Cloud and CDO to establish the management connection

- After initial establishment, CDO is used to reestablish the management connection if it is disrupted; for example, if the threat defense IP address changes due to a new DHCP assignment, CDO will inform the management center of the change.

Figure 38: Zero-Touch Provisioning Network
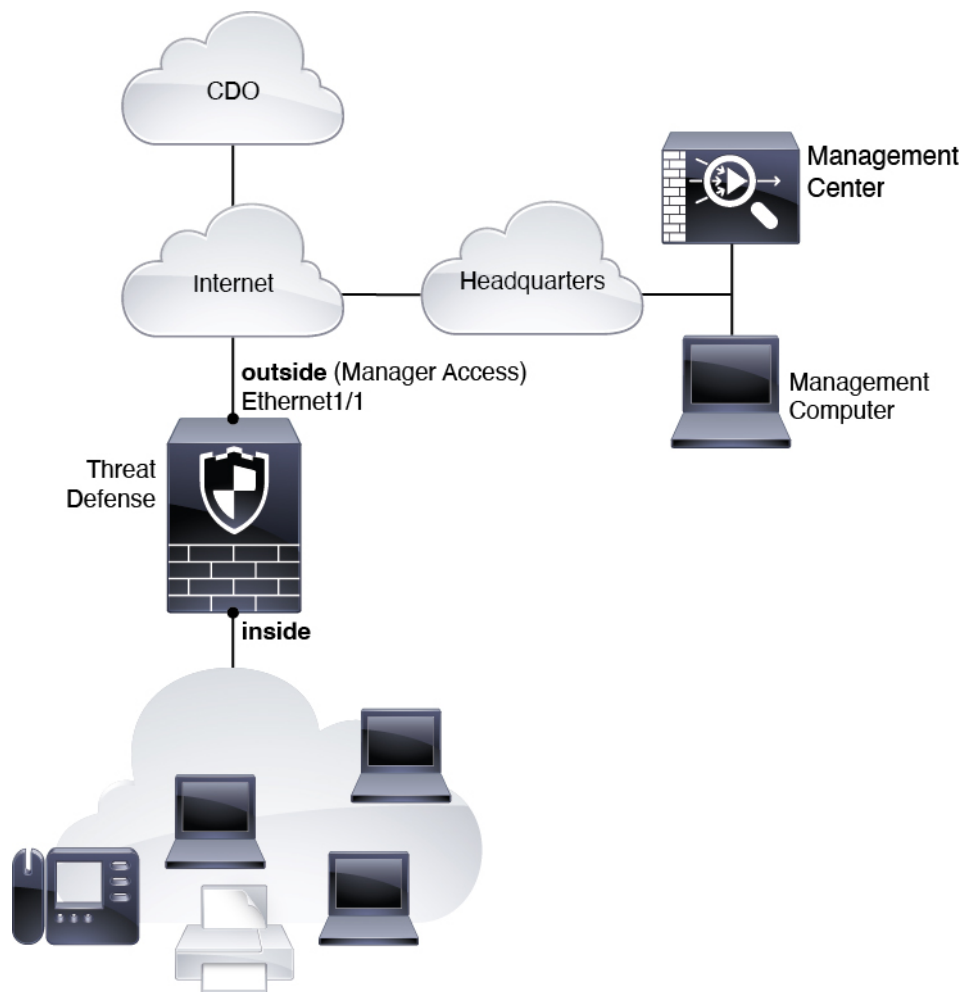
Manual Provisioning Network

The following figure shows a typical network deployment for the firewall where:

- The management center is at central headquarters.

- The threat defense uses the outside interface for manager access.

- Either the threat defense or management center needs a public IP address or hostname to allow to allow the inbound management connection; you need to know this IP address for initial setup. You can also optionally configure Dynamic DNS (DDNS) for the outside interface to accommodate changing DHCP IP assignments.

Figure 39: Manual Provisioning Network
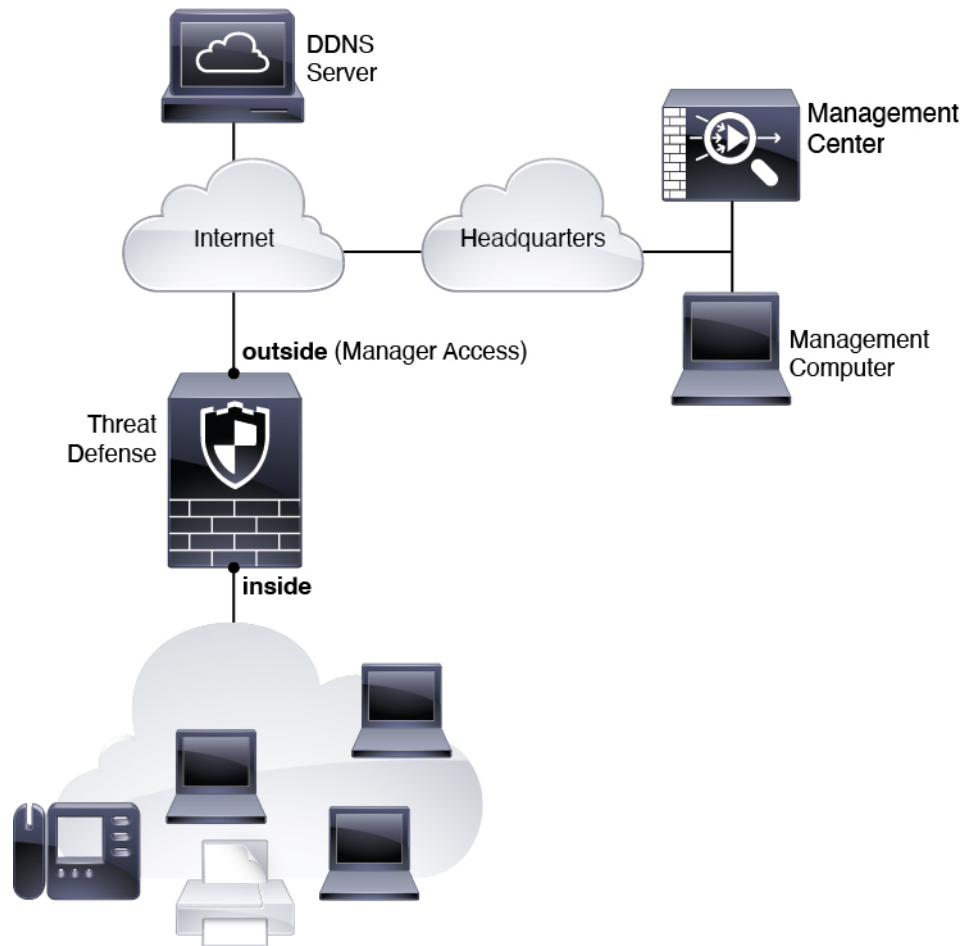
Before You Start

Deploy and perform initial configuration of the management center. See the getting started guide for your model.

End-to-End Tasks: Zero-Touch Provisioning

See the following tasks to deploy the threat defense with management center using zero-touch provisioning.

Figure 40: End-to-End Tasks: Zero-Touch Provisioning
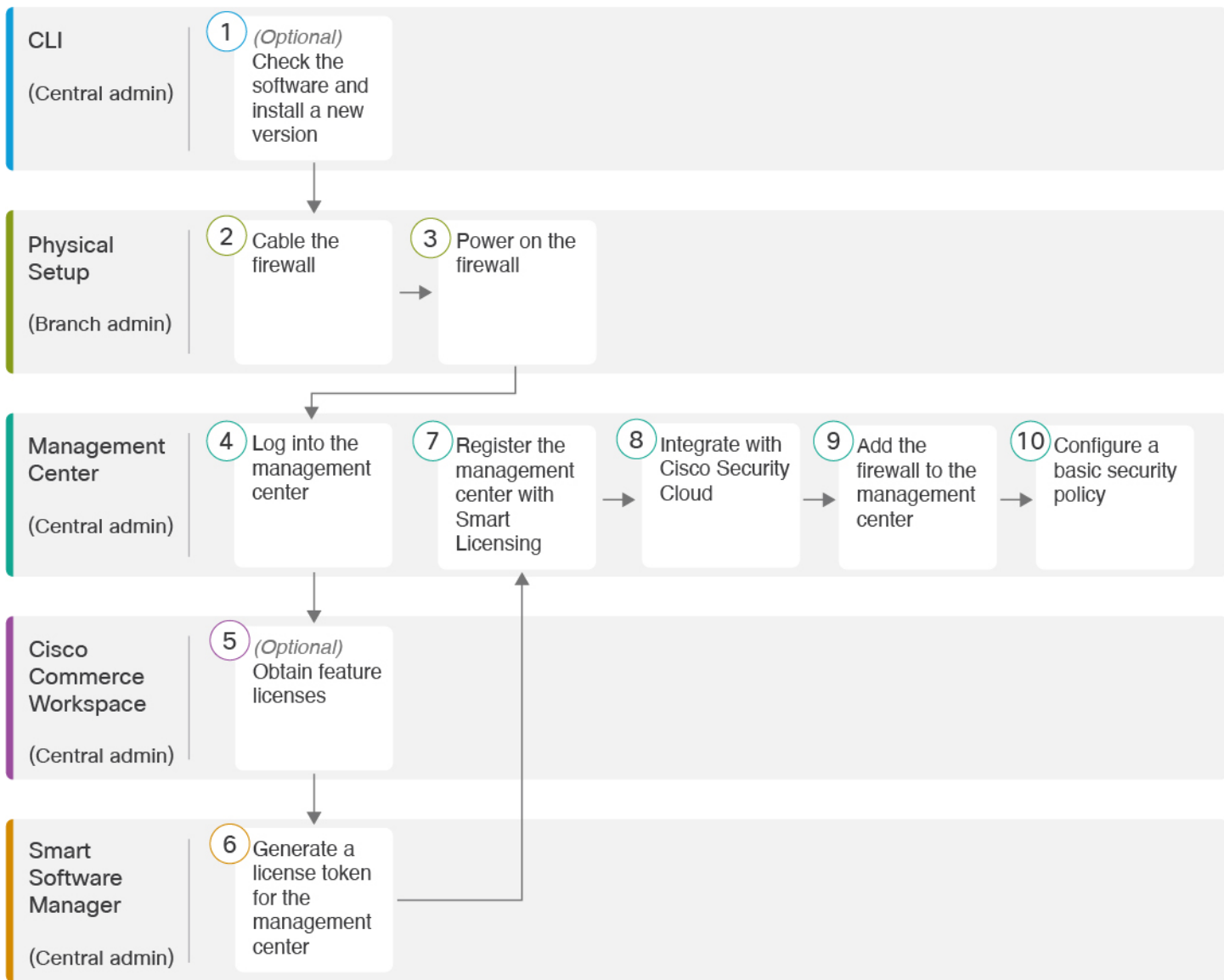
①	CLI (Central administrator)	(Optional) Check the Software and Install a New Version, on page 55.
②	Physical Setup (Branch administrator)	Cable the Firewall, on page 68.
③	Physical Setup (Branch administrator)	Power on the Firewall, on page 69.

④	Management Center (Central administrator)	Log Into the Management Center, on page 70.
⑤	Cisco Commerce Workspace (Central administrator)	Obtain Licenses for the Management Center, on page 70: Buy feature licenses.
⑥	Smart Software Manager (Central administrator)	Obtain Licenses for the Management Center, on page 70: Generate a license token for the management center.
⑦	Management Center (Central administrator)	Obtain Licenses for the Management Center, on page 70: Register the management center with the Smart Licensing server.
⑧	Management Center (Central administrator)	Add the Firewall to the Management Center Using Zero-Touch Provisioning, on page 72: Integrate the management center with Cisco Security Cloud.
⑨	Management Center (Central administrator)	Add the Firewall to the Management Center Using Zero-Touch Provisioning, on page 72
⑩	Management Center (Central administrator)	Configure a Basic Security Policy, on page 28.

End-to-End Tasks: Manual Provisioning

See the following tasks to deploy the threat defense with management center using manual provisioning.

Figure 41: End-to-End Tasks: Manual Provisioning

	CLI or Device Manager	• (Optional) Check the Software and Install a New Version, on page 55
1	(Central admin)	• Pre-Configuration Using the CLI, on page 62.
		• Pre-Configuration Using the Device Manager, on page 57
2	Physical Setup (Branch admin)	Install the firewall. See the hardware installation guide.
3	Physical Setup (Branch admin)	Cable the Firewall, on page 68.

4	Physical Setup (Branch admin)	Power on the Firewall, on page 69
5	Management Center (Central admin)	Log Into the Management Center, on page 22.
6	Cisco Commerce Workspace (Central admin)	Buy an Essentials license and optional feature licenses (Obtain Licenses for the Management Center, on page 70).
7	Smart Software Manager (Central admin)	Generate a license token for the management center (Obtain Licenses for the Management Center, on page 70).
8	Management Center (Central admin)	Register the management center with the Smart Licensing server (Obtain Licenses for the Management Center, on page 70).
9	Management Center (Central admin)	Add a Device to the Management Center Manually, on page 75.
10	Management Center (Central admin)	Configure a Basic Security Policy, on page 79.

Central Administrator Pre-Configuration

You might need to manually pre-configure the threat defense before you send it to the branch office.

(Optional) Check the Software and Install a New Version

To check the software version and, if necessary, install a different version, perform these steps. We recommend that you install your target version before you configure the firewall. Alternatively, you can perform an upgrade after you are up and running, but upgrading, which preserves your configuration, may take longer than using this procedure.

What Version Should I Run?

Cisco recommends running a Gold Star release indicated by a gold star next to the release number on the software download page. You can also refer to the release strategy described in https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html; for example, this bulletin describes short-term release numbering (with the latest features), long-term release numbering (maintenance releases and patches for a longer period of time), or extra long-term release numbering (maintenance releases and patches for the longest period of time, for government certification).

Procedure

Step 1 Connect to the console port. See Access the Threat Defense and FXOS CLI, on page 93 for more information.

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

You connect to the FXOS CLI. The first time you log in, you are prompted to change the password. This password is also used for the threat defense login for SSH.

Note   If the password was already changed, and you do not know it, you must perform a factory reset to reset the password to the default. See the FXOS troubleshooting guide for the factory reset procedure.

Example:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Step 2   At the FXOS CLI, show the running version.

scope ssa

show app-instance

Example:

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name     Slot ID     Admin State     Operational State     Running Version Startup
 Version Cluster Oper State
-------------------- ---------- --------------- -------------------- ---------------
--------------- ------------------
ftd               1          Enabled        Online               7.6.0.65       7.6.0.65
        Not Applicable
```

Step 3   If you want to install a new version, perform these steps.

a)   If you need to set a static IP address for the Management interface, see Pre-Configuration Using the CLI, on page 62. By default, the Management interface uses DHCP.

You will need to download the new image from a server accessible from the Management interface.

b)   Perform the reimage procedure in the FXOS troubleshooting guide.

After the firewall reboots, you connect to the FXOS CLI again.

c)   At the FXOS CLI, you are prompted to set the admin password again.

For zero-touch provisioning, when you onboard the device, for the **Password Reset** area, be sure to choose **No...** because you already set the password.

d) Shut down the device. See .

Perform Initial Configuration (Manual Provisioning)

For manual provisioning, perfom initial configuration of the threat defense using the CLI or using the device manager.

Pre-Configuration Using the Device Manager

When you use the device manager for initial setup, the following interfaces are preconfigured in addition to the Management interface and manager access settings:

- Ethernet 1/1—"outside", IP address from DHCP, IPv6 autoconfiguration

- Ethernet 1/2— "inside", 192.168.95.1/24

- Default route—Obtained through DHCP on the outside interface

Note that other settings, such as the DHCP server on inside, access control policy, or security zones, are not configured.

If you perform additional interface-specific configuration within device manager before registering with the management center, then that configuration is preserved.

When you use the CLI, only the Management interface and manager access settings are retained (for example, the default inside interface configuration is not retained).

Procedure

Step 1 Connect your management computer to the Inside (Ethernet 1/2) interface.

Step 2 Power on the firewall.

Note The first time you boot up the threat defense, initialization can take approximately 15 to 30 minutes.

Step 3 Log in to the device manager.
a) Enter the following URL in your browser: **https://192.168.95.1**
b) Log in with the username **admin**, and the default password **Admin123**.
c) You are prompted to read and accept the End User License Agreement and change the admin password.

Step 4 Use the setup wizard when you first log into the device manager to complete the initial configuration. You can optionally skip the setup wizard by clicking **Skip device setup** at the bottom of the page.

After you complete the setup wizard, in addition to the default configuraton for the inside interface (Ethernet1/2), you will have configuration for an outside (Ethernet1/1) interface that will be maintained when you switch to management center management.

a) Configure the following options for the outside and management interfaces and click **Next**.

1. **Outside Interface Address**—This interface is typically the internet gateway, and might be used as your manager access interface. You cannot select an alternative outside interface during initial device setup. The first data interface is the default outside interface.

If you want to use a different interface from outside (or inside) for manager access, you will have to configure it manually after completing the setup wizard.

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.

2. **Management Interface**

You will not see Management Interface settings if you performed intial setup at the CLI.

The Management interface settings are used even though you are enabling the manager access on a data interface. For example, the management traffic that is routed over the backplane through the data interface will resolve FQDNs using the Management interface DNS servers, and not the data interface DNS servers.

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.

b) Configure the **Time Setting (NTP)** and click **Next**.

1. **Time Zone**—Select the time zone for the system.

2. **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.

c) Select **Start 90 day evaluation period without registration**.

Do not register the threat defense with the Smart Software Manager; all licensing is performed on the management center.

d) Click **Finish**.

e) You are prompted to choose **Cloud Management** or **Standalone**. For management center management, choose **Standalone**, and then **Got It**.

Step 5 (Might be required) Configure the Management interface. See the Management interface on **Device** > **Interfaces**.

The Management interface must have the gateway set to data interfaces. By default, the Management interface receives an IP address and gateway from DHCP. If you do not receive a gateway from DHCP (for example, you did not connect this interface to a network), then the gateway will default to data interfaces, and you do not need to configure anything. If you did receive a gateway from DHCP, then you need to instead configure this interface with a static IP address and set the gateway to data interfaces.

Step 6 If you want to configure additional interfaces, including an interface other than outside or inside that you want to use for the manager access, choose **Device**, and then click the link in the **Interfaces** summary.

See Configure the Firewall in the Device Manager, on page 115 for more information about configuring interfaces in the device manager. Other device manager configuration will not be retained when you register the device to the management center.

Step 7 Choose **Device** > **System Settings** > **Central Management**, and click **Proceed** to set up the management center management.

Step 8 Configure the **Management Center/**CDO **Details**.

Figure 42: Management Center/CDO Details

Configure Connection to Management Center or CDO
Provide details to register to the management center/CDO.

Management Center/CDO Details
Do you know the Management Center/CDO hostname or IP address?
◉ Yes   ○ No

Threat Defense   **Management Center/CDO**

10.89.5.16   10.89.5.35
fe80::6a87:c6ff:fea6:4c00/64

Management Center/CDO Hostname or IP Address

10.89.5.35

Management Center/CDO Registration Key

●●●●   👁

NAT ID
Required when the management center/CDO hostname or IP address is not provided. We recommend always setting the NAT ID even when you specify the management center/CDO hostname or IP address.

11203

Connectivity Configuration
Threat Defense Hostname

1120-3

DNS Server Group

CustomDNSServerGroup   ⌄

Management Center/CDO Access Interface
○ Data Interface

Please select an interface   ⌄

◉ Management Interface View details

CANCEL   CONNECT

a) For **Do you know the Management Center/**CDO **hostname or IP address**, click **Yes** if you can reach the management center using an IP address or hostname, or **No** if the management center is behind NAT or does not have a public IP address or hostname.

At least one of the devices, either the management center or the threat defense device, must have a reachable IP address to establish the two-way, TLS-1.3-encrypted communication channel between the two devices.

b) If you chose **Yes**, then enter the **Management Center/**CDO **Hostname/IP Address**.

c) Specify the **Management Center/**CDO **Registration Key**.

This key is a one-time registration key of your choice that you will also specify on the management center when you register the threat defense device. The registration key must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID can be used for multiple devices registering to the management center.

d) Specify a **NAT ID**.

This ID is a unique, one-time string of your choice that you will also specify on the management center. This field is required if you only specify the IP address on one of the devices; but we recommend that you specify the NAT ID even if you know the IP addresses of both devices. The NAT ID must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID *cannot* be used for any other devices registering to the management center. The NAT ID is used in combination with the IP address to verify that the connection is coming from the correct device; only after authentication of the IP address/NAT ID will the registration key be checked.

Step 9   Configure the **Connectivity Configuration**.

a) Specify the **FTD Hostname**.

This FQDN will be used for the outside interface, or whichever interface you choose for the **Management Center/CDO Access Interface**.

b) Specify the **DNS Server Group**.

Choose an existing group, or create a new one. The default DNS group is called **CiscoUmbrellaDNSServerGroup**, which includes the OpenDNS servers.

This setting sets the *data* interface DNS server. The Management DNS server that you set with the setup wizard is used for management traffic. The data DNS server is used for DDNS (if configured) or for security policies applied to this interface. You are likley to choose the same DNS server group that you used for Management, because both management and data traffic reach the DNS server through the outside interface.

On the management center, the data interface DNS servers are configured in the Platform Settings policy that you assign to this threat defense. When you add the threat defense to the management center, the local setting is maintained, and the DNS servers are *not* added to a Platform Settings policy. However, if you later assign a Platform Settings policy to the threat defense that includes a DNS configuration, then that configuration will overwrite the local setting. We suggest that you actively configure the DNS Platform Settings to match this setting to bring the management center and the threat defense into sync.

Also, local DNS servers are only retained by the management center if the DNS servers were discovered at initial registration.

c) For the **Management Center/CDO Access Interface**, choose **outside**.

You can choose any configured interface, but this guide assumes you are using outside.

Step 10   If you chose a different data interface from outside, then add a default route.

You will see a message telling you to check that you have a default route through the interface. If you chose outside, you already configured this route as part of the setup wizard. If you chose a different interface, then you need to manually configure a default route before you connect to the management center. See Configure

the Firewall in the Device Manager, on page 115 for more information about configuring static routes in the device manager.

Step 11   Click **Add a Dynamic DNS (DDNS) method**.

DDNS ensures the management center can reach the threat defense at its Fully-Qualified Domain Name (FQDN) if the threat defense's IP address changes. See **Device** > **System Settings** > **DDNS Service** to configure DDNS.

If you configure DDNS before you add the threat defense to the management center, the threat defense automatically adds certificates for all of the major CAs from the Cisco Trusted Root CA bundle so that the threat defense can validate the DDNS server certificate for the HTTPS connection. The threat defense supports any DDNS server that uses the DynDNS Remote API specification (https://help.dyn.com/remote-access-api/).

Step 12   Click **Connect**. The **Registration Status** dialog box shows the current status of the switch to the management center. After the **Saving Management Center/**CDO **Registration Settings** step, go to the management center, and add the firewall.

If you want to cancel the switch to the management center, click **Cancel Registration**. Otherwise, do not close the device manager browser window until after the **Saving Management Center/**CDO **Registration Settings** step. If you do, the process will be paused, and will only resume when you reconnect to the device manager.

If you remain connected to the device manager after the **Saving Management Center/**CDO **Registration Settings** step, you will eventually see the **Successful Connection with Management Center or** CDO dialog box, after which you will be disconnected from the device manager.

Figure 43: Successful Connection
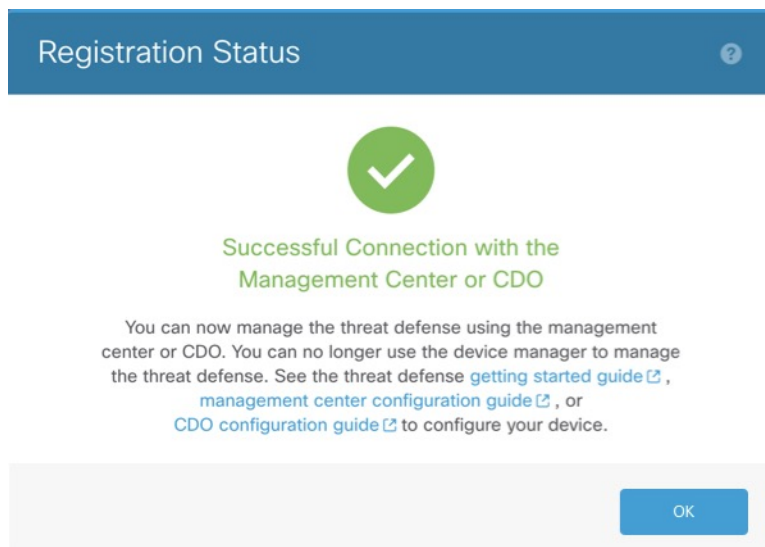
Pre-Configuration Using the CLI

Set the Management IP address, gateway, and other basic networking settings using the setup wizard. When you use the CLI for initial configuration, only the Management interface and manager access interface settings are retained. When you perform initial setup using the device manager, *all* interface configuration completed

in the device manager is retained when you switch to the management center for management, in addition to the Management interface and manager access interface settings. Note that other default configuration settings, such as the access control policy, are not retained.

Procedure

Step 1 Power on the firewall.

Note The first time you boot up the threat defense, initialization can take approximately 15 to 30 minutes.

Step 2 Connect to the threat defense CLI on the console port.

The console port connects to the FXOS CLI.

Step 3 Log in with the username **admin** and the password **Admin123**.

The first time you log in to the FXOS, you are prompted to change the password. This password is also used for the threat defense login for SSH.

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

Example:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Step 4 Connect to the threat defense CLI.

connect ftd

Example:

```
firepower# connect ftd
>
```

Step 5 The first time you log in to the threat defense, you are prompted to accept the End User License Agreement (EULA) and, if using an SSH connection, to change the admin password. You are then presented with the CLI setup script for the Management interface settings.

The Management interface settings are used even though you are enabling manager access on a data interface.

Note   You cannot repeat the CLI setup wizard 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 Cisco Secure Firewall Threat Defense Command Reference.

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

See the following guidelines:

- **Do you want to configure IPv4?** and/or **Do you want to configure IPv6?**—Enter **y** for at least one of these types of addresses. Although you do not plan to use the Management interface, you must set an IP address, for example, a private address.

- **Configure IPv4 via DHCP or manually?** and/or **Configure IPv6 via DHCP, router, or manually?**—Choose **manual**. You cannot configure a data interface for management if the management interface is set to DHCP, because the default route, which must be **data-interfaces** (see the next bullet), might be overwritten with one received from the DHCP server.

- **Enter the IPv4 default gateway for the management interface** and/or **Enter the IPv6 gateway for the management interface**—Set the gateway to be **data-interfaces**. This setting forwards management traffic over the backplane so it can be routed through the manager access data interface.

- **Manage the device locally?**—Enter **no** to use the management center. A **yes** answer means you will use the device manager instead.

- **Configure firewall mode?**—Enter **routed**. Outside manager access is only supported in routed firewall mode.

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 configure the network to continue.
Configure at least one of IPv4 or IPv6 unless managing via data interfaces.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [y]: n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.61]: 10.89.5.17
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]:
Enter a fully qualified hostname for this system [firepower]: 1010-3
Enter a comma-separated list of DNS servers or 'none'
[208.67.222.222,208.67.220.220,2620:119:35::35]:
Enter a comma-separated list of search domains or 'none' []: cisco.com
If your networking information has changed, you will need to reconnect.
Disabling IPv6 configuration: management0
Setting DNS servers: 208.67.222.222,208.67.220.220,2620:119:35::35
Setting DNS domains:cisco.com
Setting hostname as 1010-3
Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: data on management0
Updating routing tables, please wait...
All configurations applied to the system. Took 3 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'
```

```
Manage the device locally? (yes/no) [yes]: no
DHCP server is already disabled
DHCP Server Disabled
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...


Device is in OffBox mode - disabling/removing port 443 from iptables.
Update policy deployment information
    - add device configuration
    - add network discovery
    - add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required.  In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>
```

Step 6   Configure the outside interface for manager access.

configure network management-data-interface

You are then prompted to configure basic network settings for the outside interface. See the following details for using this command:

- The Management interface cannot use DHCP if you want to use a data interface for management. If you did not set the IP address manually during initial setup, you can set it beforehand using the **configure network** {**ipv4** | **ipv6**} **manual** command. If you did not already set the Management interface gateway to **data-interfaces**, this command will set it now.

- When you add the threat defense to the management center, the management center discovers and maintains the interface configuration, including the following settings: interface name and IP address, static route to the gateway, DNS servers, and DDNS server. For more information about the DNS server configuration, see below. In the management center, you can later make changes to the manager access interface configuration, but make sure you don't make changes that can prevent the threat defense or the management center from re-establishing the management connection. If the management connection is disrupted, the threat defense includes the **configure policy rollback** command to restore the previous deployment.

- If you configure a DDNS server update URL, the threat defense automatically adds certificates for all of the major CAs from the Cisco Trusted Root CA bundle so that the threat defense can validate the DDNS server certificate for the HTTPS connection. The threat defense supports any DDNS server that uses the DynDNS Remote API specification (https://help.dyn.com/remote-access-api/).

- This command sets the *data* interface DNS server. The Management DNS server that you set with the setup script (or using the **configure network dns servers** command) is used for management traffic. The data DNS server is used for DDNS (if configured) or for security policies applied to this interface.

  On the management center, the data interface DNS servers are configured in the Platform Settings policy that you assign to this threat defense. When you add the threat defense to the management center, the local setting is maintained, and the DNS servers are *not* added to a Platform Settings policy. However, if you later assign a Platform Settings policy to the threat defense that includes a DNS configuration, then that configuration will overwrite the local setting. We suggest that you actively configure the DNS Platform Settings to match this setting to bring the management center and the threat defense into sync.

  Also, local DNS servers are only retained by the management center if the DNS servers were discovered at initial registration. For example, if you registered the device using the Management interface, but then later configure a data interface using the **configure network management-data-interface** command, then you must manually configure all of these settings in the management center, including the DNS servers, to match the threat defense configuration.

- You can change the management interface after you register the threat defense to the management center, to either the Management interface or another data interface.

- The FQDN that you set in the setup wizard will be used for this interface.

- You can clear the entire device configuration as part of the command; you might use this option in a recovery scenario, but we do not suggest you use it for initial setup or normal operation.

- To disable data managemement, enter the **configure network management-data-interface disable** command.

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://dwinchester:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:
```

```
Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Step 7   (Optional) Limit data interface access to the management center on a specific network.

configure network management-data-interface client *ip_address netmask*

By default, all networks are allowed.

Step 8   Identify the management center that will manage this threat defense.

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *reg_key* [*nat_id*]

- • {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**}—Specifies either the FQDN or IP address of the management center. If the management center is not directly addressable, use **DONTRESOLVE**. At least one of the devices, either the management center or the threat defense, must have a reachable IP address to establish the two-way, SSL-encrypted communication channel between the two devices. If you specify **DONTRESOLVE** in this command, then the threat defense must have a reachable IP address or hostname.

- • *reg_key*—Specifies a one-time registration key of your choice that you will also specify on the management center when you register the threat defense. The registration key must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-).

- • *nat_id*—Specifies a unique, one-time string of your choice that you will also specify on the management center. When you use a data interface for management, then you must specify the NAT ID on *both* the threat defense and the management center for registration. The NAT ID must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID cannot be used for any other devices registering to the management center.

Example:

```
> configure manager add fmc-1.example.com regk3y78 natid56
Manager successfully configured.
```

Step 9   Shut down the threat defense so you can send the device to the remote branch office.

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 system.

a) Enter the **shutdown** command.
b) Observe the Power LED and Status LED to verify that the chassis is powered off (appear unlit).
c) After the chassis has successfully powered off, you can then unplug the power to physically remove power from the chassis if necessary.

Branch Office Installation

After you receive the threat defense from central headquarters, you only need to cable and power on the firewall so that it has internet access from the outside interface. The central administrator can then complete the configuration.

Cable the Firewall

The management center and your management computer reside at a remote headquarters and can reach the threat defense over the internet. To cable the Secure Firewall 3100, see the following steps.

Figure 44: Cabling a Remote Management Deployment

Before you begin

(Optional) Obtain a console adapter—The Secure Firewall 3100 ships with a DB-9 to RJ-45 serial cable, so you may need to buy a third party DB-9-to-USB serial cable to make the connection.

Procedure

Step 1   Install the chassis. See the hardware installation guide.

Step 2   Connect the outside interface (Ethernet 1/1) to your outside router.

Step 3   Connect the inside interface (for example, Ethernet 1/2) to your inside switch or router.

You can choose any interface for inside.

Step 4   Connect other networks to the remaining interfaces.

Step 5   (Optional) Connect the management computer to the console port.

At the branch office, the console connection is not required for everyday use; however, it may be required for troubleshooting purposes.

Power on the Firewall

System power is controlled by a rocker power switch located on the rear of the firewall. The power switch is implemented as a soft notification switch that supports graceful shutdown of the system to reduce the risk of system software and data corruption.

Note   The first time you boot up the threat defense, initialization can take approximately 15 to 30 minutes.

Before you begin

It's important that you provide reliable power for your firewall (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 firewall, 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 back of the firewall; if it is solid green, the firewall is powered on.

Figure 45: System and Power LEDs
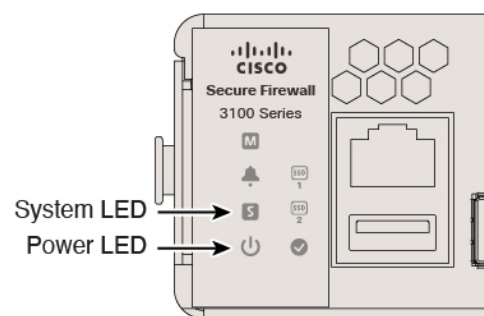
Step 4   Check the System LED on the back of the firewall; after it is solid green, the system has passed power-on diagnostics.

Note   When the switch is toggled from ON to OFF, it may take several seconds for the system to eventually power off. During this time, the Power LED on the front of the chassis blinks green. Do not remove the power until the Power LED is completely off.

Central Administrator Post-Configuration

After the remote branch administrator cables the threat defense so it has internet access from the outside interface, you can register the threat defense to the management center and complete configuration of the device.

Log Into the Management Center

Use the management center to configure and monitor the threat defense.

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 Management Center

All licenses are supplied to the threat defense by the management center. You can optionally purchase the following feature licenses:

- **Essentials**—(Required) Essentials license.

- **IPS**—Security Intelligence and Next-Generation IPS

- **Malware Defense**—Malware defense

- **URL Filtering**—URL Filtering

- **Cisco Secure Client**—Secure Client Advantage, Secure Client Premier, or Secure Client VPN Only

- **Carrier**—Diameter, GTP/GPRS, M3UA, SCTP

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

Before you begin

- Have an 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 an 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 **Search All** field on the Cisco Commerce Workspace.

Figure 46: License Search
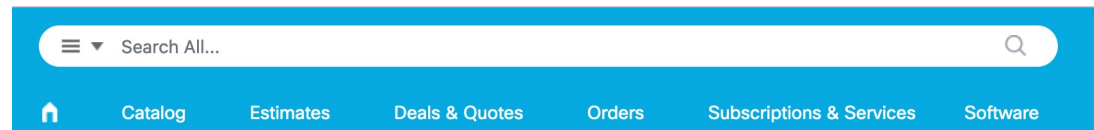
Choose **Products & Services** from the results.

Figure 47: Results

Search for the following license PIDs:

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

• Essentials:

  • *Included automatically*

• IPS, Malware Defense, and URL license combination:

  • L-FPR3110T-TMC=

  • L-FPR3120T-TMC=

  • L-FPR3130T-TMC=

  • L-FPR3140T-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-FPR3110T-TMC-1Y

           • L-FPR3110T-TMC-3Y

           • L-FPR3110T-TMC-5Y

           • L-FPR3120T-TMC-1Y

           • L-FPR3120T-TMC-3Y

           • L-FPR3120T-TMC-5Y

           • L-FPR3130T-TMC-1Y

           • L-FPR3130T-TMC-3Y

           • L-FPR3130T-TMC-5Y

           • L-FPR3140T-TMC-1Y

           • L-FPR3140T-TMC-3Y

           • L-FPR3140T-TMC-5Y

       • Carrier license:

           • L-FPR3K-FTD-CAR=

       • Cisco Secure Client—See the Cisco Secure Client Ordering Guide.

Step 2   If you have not already done so, register the management center with the Smart Software Manager.

Registering requires you to generate a registration token in the Smart Software Manager. See the management center configuration guide for detailed instructions.

Register the Threat Defense with the Management Center

Register the threat defense with the management center depending on which deployment method you are using.

Add the Firewall to the Management Center Using Zero-Touch Provisioning

Zero-Touch Provisioning lets you register devices to the management center by serial number without having to perform any initial setup on the device. The management center integrates with the Cisco Security Cloud and Cisco Defense Orchestrator (CDO) for this functionality.

When you use zero-touch provisioning, the following interfaces are preconfigured. Note that other settings, such as the DHCP server on inside, access control policy, or security zones, are not configured.

       • Ethernet 1/1—"outside", IP address from DHCP, IPv6 autoconfiguration

       • Ethernet 1/2 (or for the , the VLAN1 interface)— "inside", 192.168.95.1/24

       • Default route—Obtained through DHCP on the outside interface

Zero-Touch Provisioning is not supported with clustering or multi-instance mode.

High availability is only supported when you use the Management interface because zero-touch provisioning uses DHCP, which is not supported for data interfaces and high availability.

Note For management center version 7.4, you need to add the device using CDO; see the 7.4 guide for more information. The native management center workflow was added in 7.6. Also, for cloud integration in 7.4, see the **SecureX Integration** page in the management center.

Before you begin

- If the device does not have a public IP address or FQDN, set a public IP address/FQDN for the management center (for example, if it is behind NAT), so the device can initiate the management connection. See .

Procedure

Step 1 The first time you add a device using a serial number, integrate the management center with Cisco Security Cloud.

Note For a management center high-availability pair, you also need to integrate the secondary management center with Cisco Security Cloud.

a) Choose **Integration** > **Cisco Security Cloud**.

b) Click **Enable Cisco Security Cloud** to open a separate browser tab to log you into your Cisco Security Cloud account and confirm the displayed code.

Make sure this page is not blocked by a pop-up blocker. If you do not already have a Cisco Security Cloud and CDO account, you can add one during this procedure.

For detailed information about this integration, see .

CDO onboards the on-prem management center after you integrate the management center with Cisco Security Cloud. CDO needs the management center in its inventory for zero-touch provisioning to operate. However, you do not need to use CDO directly. If you do use CDO, its management center support is limited to device onboarding, viewing its managed devices, viewing objects associated with the management center, and cross-launching the management center.

c) Make sure **Enable Zero-Touch Provisioning** is checked.

d) Click **Save**.

Step 2 Choose **Devices** > **Device Management**.

Step 3 From the **Add** drop-down menu, choose **Device (Wizard)**.

Step 4 Click **Use Serial Number**, and then click **Next**.

Figure 48: Device Registration Method

Step 5   For the **Initial device configuration**, click the **Basic** radio button.

Figure 49: Initial Device Configuration Method

a)   Choose an initial **Access Control Policy** to deploy to the device upon registration, or create a new policy.

If the device is incompatible with the policy you choose, deploying will fail. This incompatibility could occur for multiple reasons, including licensing mismatches, model restrictions, passive vs inline issues, and other misconfigurations. After you resolve the issue that caused the failure, manually deploy configurations to the device.

b)   Choose **Smart licensing** licenses to apply to the device.

You can also apply licenses after you add the device, from the **System** > **Licenses** > **Smart Licenses** page.

c)   Click **Next**.

Step 6   Configure the **Device details**.

Figure 50: Device details

Add Device ⑦

① **Device registration method**

　Device registration method **Serial Number**

② **Initial device configuration**

　Access control policy **wfx_automationPolicy123**

③ **Device details**

ⓘ Configure the public IP address or FQDN for the Management Center, except in scenarios where the Threat Defense device is publicly reachable, running a version earlier than 7.4, and is connected to the data interface. To configure the public IP address or FQDN, go to Configuration > Manager Remote Access.

Serial number | Display name
JAD25440DW1 | FTD1

Device group
Select...   ⌄

Set the device password
Enter a new password if you have not previously changed the device's default password.

New password | Confirm password
•••••••• | ••••••••

Skip this field if you already changed the password on the device. If you provide a new password in this case, registration will fail.

Previous

Cancel   　Add Device

a) Enter the **Serial number**.
b) Enter the **Display name** as you want it to display in the management center
c) (Optional) Choose the **Device Group**.
d) **Set the device password**.

　　If this device is unconfigured or a fresh install, then you need to set a new password. If you already logged in and changed the password, then leave this field blank. Otherwise, registration will fail.

Step 7   Click **Add Device**.

It may take up to two minutes for the management center to verify the device's heartbeat and establish communication. If the registration succeeds, the device is added to the list.

Add a Device to the Management Center Manually

Register the threat defense to the management center manually using the device IP address or hostname and registration key.

Procedure

Step 1 In the management center, choose **Devices** > **Device Management**.

Step 2 From the **Add** drop-down list, choose **Add Device**.

Figure 51: Add Device Using a Registration Key

Add Device ⊙

☐ CDO Managed Device

Host:†

10.89.5.41

Display Name:

3110-1

Registration Key:*

••••

Group:

None

Access Control Policy:*

wfx_automationPolicy123

Smart Licensing
Note: All virtual Firewall Threat Defense devices require a performance tier license.
Make sure your Smart Licensing account contains the available licenses you need.
It's important to choose the tier that matches the license you have in your account.
Click here for information about the Firewall Threat Defense performance-tiered licensing.
Until you choose a tier, your Firewall Threat Defense virtual defaults to the FTDv50 selection.

Performance Tier (only for Firewall Threat Defense virtual 7.0 and above):

Select a recommended Tier

☑ Carrier
☑ Malware Defense
☑ IPS
☑ URL

Advanced
Unique NAT ID:†

31101

☑ Transfer Packets

Cancel   **Register**

Figure 52: Add Device

Set the following parameters:

- **Host**—Enter the IP address or hostname of the threat defense you want to add. You can leave this field blank if you specified both the management center IP address and a NAT ID in the threat defense initial configuration.

   Note In an HA environment, when both the management centers are behind a NAT, you can register the threat defense without a host IP or name in the primary management center. However, for registering the threat defense in a secondary management center, you must provide the IP address or hostname for the threat defense.

- **Display Name**—Enter the name for the threat defense as you want it to display in the management center.

- **Registration Key**—Enter the same registration key that you specified in the threat defense initial 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 40.

Figure 53: New Policy

New Policy ⓘⓘⓘ ⑦

Name:

[ftd-ac-policy|]

Description:

[   ]

Select Base Policy:

[None   ▾]

Default Action:

◉ Block all traffic
◯ Intrusion Prevention
◯ Network Discovery

[Cancel] [**Save**]

- **Smart Licensing**—Assign the Smart Licenses you need for the features you want to deploy. **Note:** You can apply the Secure Client remote access VPN license after you add the device, from the **System** > **Licenses** > **Smart Licenses** page.

- **Unique NAT ID**—Specify the NAT ID that you specified in the threat defense initial configuration.

- **Transfer Packets**—Allow the device to transfer packets to the management center. When events like IPS or Snort are triggered with this option enabled, the device sends event metadata information and packet data to the management center for inspection. If you disable it, only event information will be sent to the management center, 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 threat defense fails to register, check the following items:

- Ping—Access the threat defense CLI, and ping the management center 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 threat defense Management IP address, use the **configure network management-data-interface** command.

- Registration key, NAT ID, and management center 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 threat defense using the **configure manager add** command.

For more troubleshooting information, see https://cisco.com/go/fmc-reg-error.

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. You configured basic settings for the outside interface as part of the manager access setup, but you still need to assign it to a security zone.

- DHCP server—Use a DHCP server on the inside interface for clients.

- NAT—Use interface PAT on the outside interface.

- Access control—Allow traffic from inside to outside.

- SSH—Enable SSH on the manager access interface.

Configure Interfaces

When you use zero-touch provisioning or the device manager for initial setup, the following interfaces are preconfigured:

- Ethernet 1/1—"outside", IP address from DHCP, IPv6 autoconfiguration

- Ethernet 1/2— "inside", 192.168.95.1/24

- Default route—Obtained through DHCP on the outside interface

If you performed additional interface-specific configuration within device manager before registering with the management center, then that configuration is preserved.

In any case, you need to perform additional interface configuration after you register the device. Enable the threat defense interfaces, assign them to security zones, and set the IP addresses. Also configure breakout 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 **Edit** (✎) for the firewall.

Step 2   Click **Interfaces**.

Figure 54: Interfaces

Step 3   To create 4 x 10-Gb breakout interfaces from a 40-Gb interface (available on some models), click the breakout icon for the interface.

If you already used the 40-Gb interface in your configuration, you will have to remove the configuration before you can proceed with the breakout.

Step 4   Click **Edit** (✎) for the interface that you want to use for *inside*.

The **General** tab appears.

Figure 55: General Tab

Edit Physical Interface

| General | IPv4 | IPv6 | Path Monitoring | H |

Name:

inside

☑ Enabled

☐ Management Only

Description:

Mode:

None ▼

Security Zone:

inside_zone ▼

Interface ID:

GigabitEthernet0/1

MTU:

1500

(64 - 9000)

Priority:

0   *(0 - 65535)*

Propagate Security Group Tag: ☐

NVE Only:

☐

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**

Figure 56: IPv4 Tab

Edit Physical Interface

| General | IPv4 | IPv6 | Path Monitoring |

IP Type:

Use Static IP ▼

IP Address:

192.168.1.1/24

eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

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

Figure 57: IPv6 Tab

Edit Physical Interface

| General | IPv4 | IPv6 | Path Monitoring | Hardware Configu |

| Basic | Address | Prefixes | Settings | DHCP |

Enable IPV6: ☐

Enforce EUI 64: ☐

Link-Local address: [   ]

Autoconfiguration: ☑

Obtain Default Route: ☐

f) Click **OK**.

Step 5 Click **Edit** (✎) for the interface that you want to use for *outside*.

The **General** tab appears.

Figure 58: General Tab

Edit Physical Interface

| General | IPv4 | IPv6 | Path Monitoring | Hardware |

Name:

outside

☑ Enabled

☐ Management Only

Description:

Mode:

None ▼

Security Zone:

outside_zone ▼

Interface ID:

GigabitEthernet0/0

MTU:

1500

(64 - 9000)

Priority:

0   *(0 - 65535)*

Propagate Security Group Tag: ☐

NVE Only:

☐

You already pre-configured this interface for manager access, so the interface will already be named, enabled, and addressed. You should not alter any of these basic settings because doing so will disrupt the management center management connection. You must still configure the Security Zone on this screen for through traffic policies.

a) 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**.

b) Click **OK**.

Step 6   Click **Save**.

Configure the DHCP Server

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

Procedure

Step 1   Choose **Devices** > **Device Management**, and click **Edit** (✎) for the device.

Step 2   Choose **DHCP** > **DHCP Server**.

Figure 59: DHCP Server

Step 3   On the **Server** page, click **Add**, and configure the following options:

Figure 60: Add Server

- **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**.

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**.

Figure 61: New Policy

The policy is added the management center. You still have to add rules to the policy.

Figure 62: NAT Policy
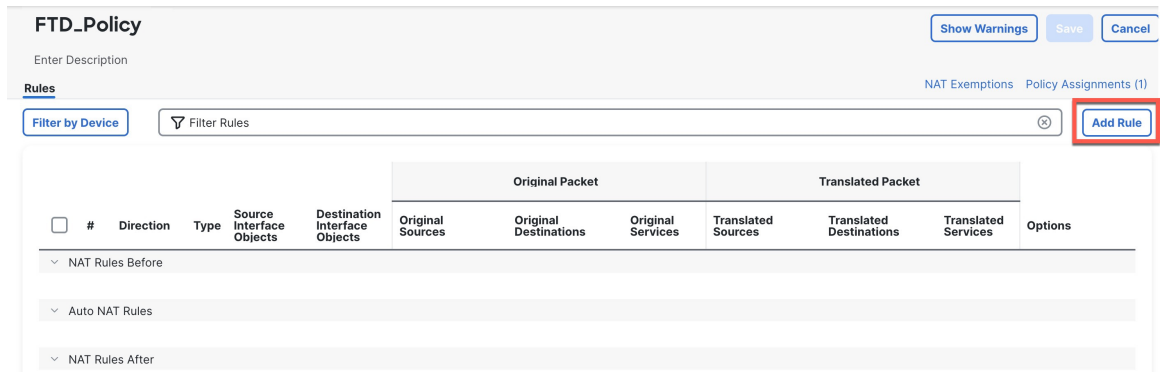
Step 3   Click **Add Rule**.

The **Add NAT Rule** dialog box appears.

Step 4   Configure the basic rule options:

Figure 63: Basic Rule Options
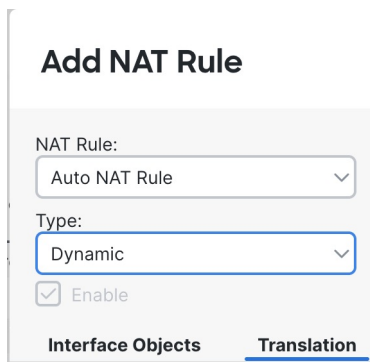
- **NAT Rule**—Choose **Auto NAT Rule**.

- **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.

Figure 64: Interface Objects

Step 6   On the **Translation** page, configure the following options:

Figure 65: Translation

Interface Objects	Translation	PAT Pool	Advanced

Original Packet

Original Source:*

all-ipv4   +

Original Port:

TCP

Translated Packet

Translated Source:

Destination Interface IP

ⓘ The values selected for Destination Interface Objects in 'Interface Objects' tab will be used

Translated Port:

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

Figure 66: New Network Object

New Network Object   ⑦

Name

all-ipv4

Description

Network

○ Host   ○ Range   ● Network   ○ FQDN

0.0.0.0/0

☐ **Allow Overrides**

Cancel   **Save**

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 threat defense, 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.

Procedure

Step 1 Choose **Policy** > **Access Policy** > **Access Policy**, and click **Edit** (✎) for the access control policy assigned to the threat defense.

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

Figure 67: Source Zone
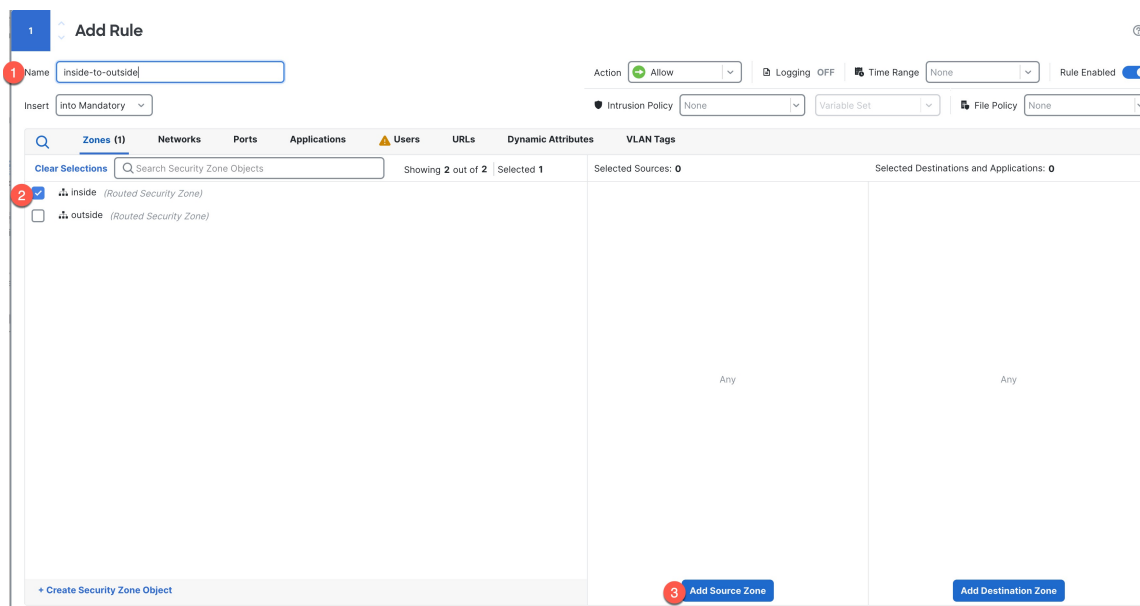
Figure 68: Destination Zone

Figure 69: Apply

- **Name**—Name this rule, for example, **inside-to-outside**.

- **Selected Sources**—Select the inside zone from **Zones**, and click **Add Source Zone**.

- **Selected Destinations and Applications**—Select the outside zone from **Zones**, and click **Add Destination Zone**.

Leave the other settings as is.

Step 3   Click **Apply**.

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

Step 4   Click **Save**.

Configure SSH on the Manager Access Data Interface

If you enabled management center access on a data interface, such as outside, you should enable SSH on that interface using this procedure. This section describes how to enable SSH connections to one or more *data* interfaces on the threat defense. SSH is not supported to the Diagnostic logical interface.

The threat defense uses the CiscoSSH stack, which is based on OpenSSH. CiscoSSH supports FIPS compliance and regular updates, including updates from Cisco and the open source community.

Note   SSH is enabled by default on the Management interface; however, this screen does not affect Management SSH access.

The Management interface is separate from the other interfaces on the device. It is used to set up and register the device to the management center. SSH for data interfaces shares the internal and external user list with SSH for the Management interface. Other settings are configured separately: for data interfaces, enable SSH and access lists using this screen; SSH traffic for data interfaces uses the regular routing configuration, and not any static routes configured at setup or at the CLI.

For the Management interface, to configure an SSH access list, see the **configure ssh-access-list** command in the Cisco Secure Firewall Threat Defense Command Reference. To configure a static route, see the **configure network static-routes** command. By default, you configure the default route through the Management interface at initial setup.

To use SSH, you do not also need an access rule allowing the host IP address. You only need to configure SSH access according to this section.

You can SSH only to a reachable interface (including an interface in a user-defined virtual router); if your SSH host is located on the outside interface, you can only initiate a management connection directly to the outside interface. When you enable SSH in a user-defined virtual router, and you want VPN users to access SSH, be sure to terminate the VPN on the same virtual router. If the VPN is terminated on another virtual router, then you must configure route leaks between the virtual routers.

SSH supports the following ciphers and key exchange:

- Encryption—aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr

- Integrity—hmac-sha2-256

- Key exchange—dh-group14-sha256

Note   After you make three consecutive failed attempts to log into the CLI using SSH, the device terminates the SSH connection.

Before you begin

- You can configure SSH internal users at the CLI using the **configure user add** command. By default, there is an **admin** user for which you configured the password during initial setup. You can also configure external users on LDAP or RADIUS by configuring **External Authentication** in platform settings.

- You need network objects that define the hosts or networks you will allow to make SSH connections to the device. You can add objects as part of the procedure, but if you want to use object groups to identify a group of IP addresses, ensure that the groups needed in the rules already exist. Select **Objects** > **Object Management** to configure objects.

✎

| **Note** | You cannot use the system-provided **any** network object. Instead, use **any-ipv4** or **any-ipv6**. |

Procedure

Step 1   Choose **Devices** > **Platform Settings** and create or edit the threat defense policy.

Step 2   Select **Secure Shell**.

Step 3   Identify the interfaces and IP addresses that allow SSH connections.

Use this table to limit which interfaces will accept SSH connections, and the IP addresses of the clients who are allowed to make those connections. You can use network addresses rather than individual IP addresses.

a)   Click **Add** to add a new rule, or click **Edit** to edit an existing rule.

b)   Configure the rule properties:

- **IP Address**—The network object or group that identifies the hosts or networks you are allowing to make SSH connections. Choose an object from the drop-down menu, or click + to add a new network object.

- **Security Zones**—Add the zones that contain the interfaces to which you will allow SSH connections. For interfaces not in a zone, you can type the interface name into the field below the **Selected Security Zones** list and click **Add**. These rules will be applied to a device only if the device includes the selected interfaces or zones.

c)   Click **OK**.

Step 4   Click **Save**.

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

Deploy the Configuration

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

Procedure

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

Figure 70: Deploy
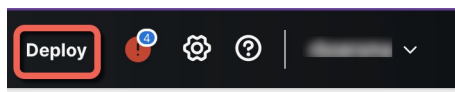
Step 2 For a quick deployment, check specific devices and then click **Deploy**, or click **Deploy All** to deploy to all devices. Otherwise, for additional deployment options, click **Advanced Deploy**.

Figure 71: Deploy Selected
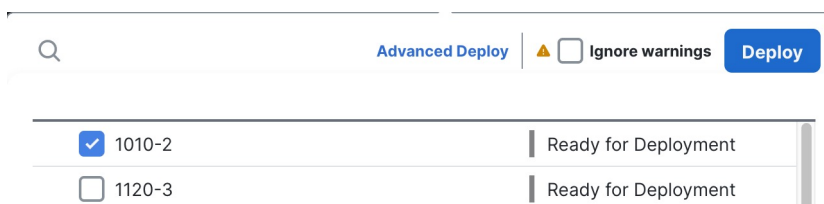
Figure 72: Deploy All
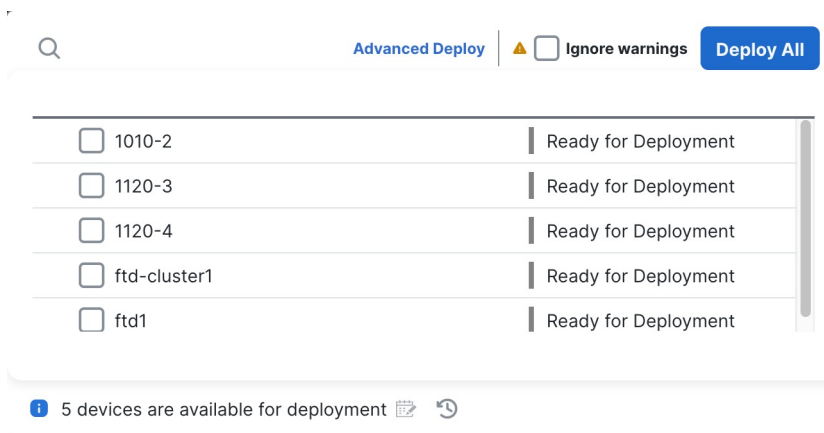
Figure 73: Advanced Deploy

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.

Figure 74: Deployment Status

Access the Threat Defense and FXOS 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 also access the FXOS CLI for troubleshooting purposes.

Note You can alternatively SSH to the Management interface of the threat defense device. Unlike a console session, the SSH session defaults to the threat defense CLI, from which you can connect to the FXOS CLI using the **connect fxos** command. You can later 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. This procedure describes console port access, which defaults to the FXOS CLI.

Procedure

Step 1 To log into the CLI, connect your management computer to the console port. The Secure Firewall 3100 ships with a DB-9 to RJ-45 serial cable, so you may need to buy a third party DB-9-to-USB serial cable to make the connection. Be sure to install any necessary USB serial drivers for your operating system. The console port defaults to the FXOS CLI. Use the following serial settings:

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

You connect to the FXOS CLI. Log in to the CLI using the **admin** username and the password you set at initial setup (the default is **Admin123**).

Example:

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

Step 2 Access the threat defense CLI.

connect ftd

Example:

```
firepower# connect ftd
>
```

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

Step 3 To exit the threat defense CLI, enter the **exit** or **logout** command.

This command returns you to the FXOS CLI prompt. For information on the commands available in the FXOS CLI, enter **?**.

Example:

```
> exit
firepower#
```

Power Off the Firewall

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 firewall system.

You can power off the device using the management center device management page, or you can use the FXOS CLI.

Power Off the Firewall Using the Management Center

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 firewall.

You can shut down your system properly using the management center.

Procedure

Step 1   Choose **Devices** > **Device Management**.

Step 2   Next to the device that you want to restart, click **Edit** (✎).

Step 3   Click the **Device** tab.

Step 4   Click **Shut Down Device** (✖) in the **System** section.

Step 5   When prompted, confirm that you want to shut down the device.

Step 6   If you have a console connection to the firewall, monitor the system prompts as the firewall shuts down. You will see the following prompt:

```
System is stopped.
It is safe to power off now.

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

If you do not have a console connection, wait approximately 3 minutes to ensure the system has shut down.

Step 7   You can now turn off the power switch and unplug the power to physically remove power from the chassis if necessary.

Power Off the Firewall at the CLI

You can use the FXOS CLI to safely shut down the system and power off the device. You access the CLI by connecting to the console port; see .

Procedure

Step 1 In the FXOS CLI, connect to local-mgmt:

firepower # **connect local-mgmt**

Step 2 Issue the **shutdown** command:

firepower(local-mgmt) # **shutdown**

Example:

```
firepower(local-mgmt)# shutdown
This command will shutdown the system.  Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense......ok
```

Step 3 Monitor the system prompts as the firewall shuts down. You will see the following prompt:

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

Step 4 You can now turn off the power switch and unplug the power to physically remove power from the chassis if necessary.

What's Next?

To continue configuring your threat defense, see the documents available for your software version at Navigating the Cisco Secure Firewall Threat Defense Documentation.

For information related to using the management center, see the Cisco Secure Firewall Management Center Device Configuration Guide.

CHAPTER 4

Threat Defense Deployment with the Device Manager

Is This Chapter for You?

To see all available applications and managers, see Which Application and Manager is Right for You?, on page 1. This chapter applies to the threat defense with the device manager.

About the Firewall

The hardware can run either threat defense software or ASA software. Switching between threat defense and ASA requires you to reimage the device. You should also reimage if you need a different software version than is currently installed. See Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.

The firewall runs an underlying operating system called the Secure Firewall eXtensible Operating System (FXOS). The firewall does not support the FXOS Secure Firewall chassis manager; only a limited CLI is supported for troubleshooting purposes. See the Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 and Secure Firewall 3100/4200 with Firepower Threat Defense for more information.

Privacy Collection Statement—The firewall 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 Tasks, on page 98
- Review the Network Deployment and Default Configuration, on page 99
- Cable the Firewall, on page 101
- Power on the Firewall, on page 102
- (Optional) Check the Software and Install a New Version, on page 103
- (Optional) Change Management Network Settings at the CLI, on page 105
- Log Into the Device Manager, on page 107
- Complete the Initial Configuration, on page 107
- Configure Licensing, on page 109
- Configure the Firewall in the Device Manager, on page 115
- Access the Threat Defense and the FXOS CLI, on page 118
- Power Off the Firewall, on page 120
- What's Next?, on page 121

End-to-End Tasks

See the following tasks to deploy the threat defense with the device manager on your chassis.

Figure 75: End-to-End Procedure
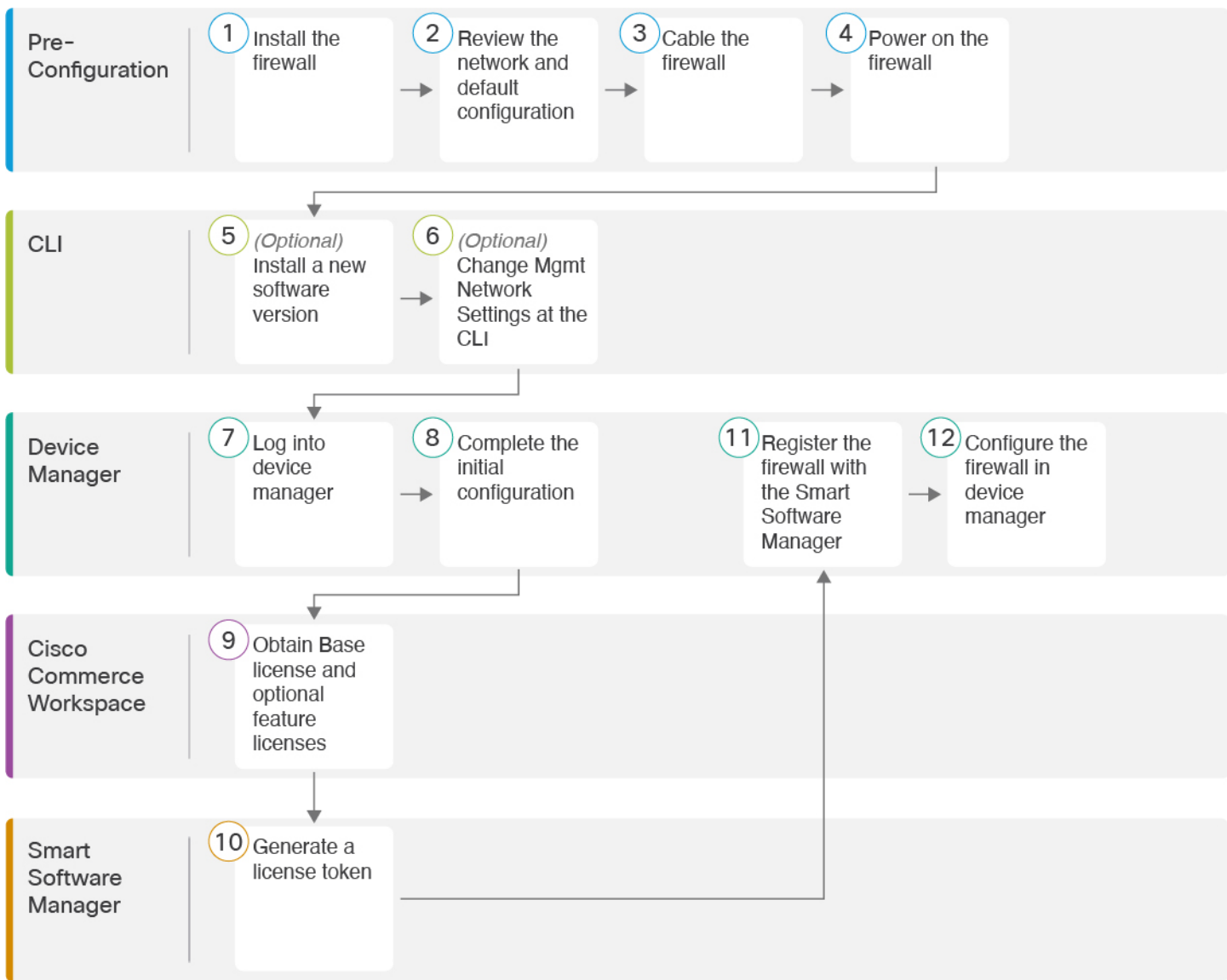
①	Pre-Configuration	Install the firewall. See the hardware installation guide.
②	Pre-Configuration	Review the Network Deployment and Default Configuration, on page 99.
③	Pre-Configuration	Cable the Firewall, on page 101.

④	Pre-Configuration	Power on the Firewall, on page 102.
⑤	CLI	(Optional) Check the Software and Install a New Version, on page 103.
⑥	CLI	(Optional) Change Management Network Settings at the CLI, on page 105.
⑦	Device Manager	Log Into the Device Manager, on page 107.
⑧	Device Manager	Complete the Initial Configuration, on page 107.
⑨	Cisco Commerce Workspace	Obtain the Base license and optional feature licenses (Configure Licensing, on page 109).
⑩	Smart Software Manager	Generate a license token (Configure Licensing, on page 109).
⑪	Device Manager	Register the firewall with the Smart Licensing Server (Configure Licensing, on page 109).
⑫	Device Manager	Configure the Firewall in the Device Manager, on page 115.

Review the Network Deployment and Default Configuration

You can manage the threat defense using the device manager 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 threat defense 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 device manager.

✎

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 the device manager. For example, you may need to change the inside IP address in the following circumstances:

- The inside IP address is 192.168.95.1.

- If you add the threat defense 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 the threat defense using the device manager with the default configuration.

Figure 76: Suggested Network Deployment
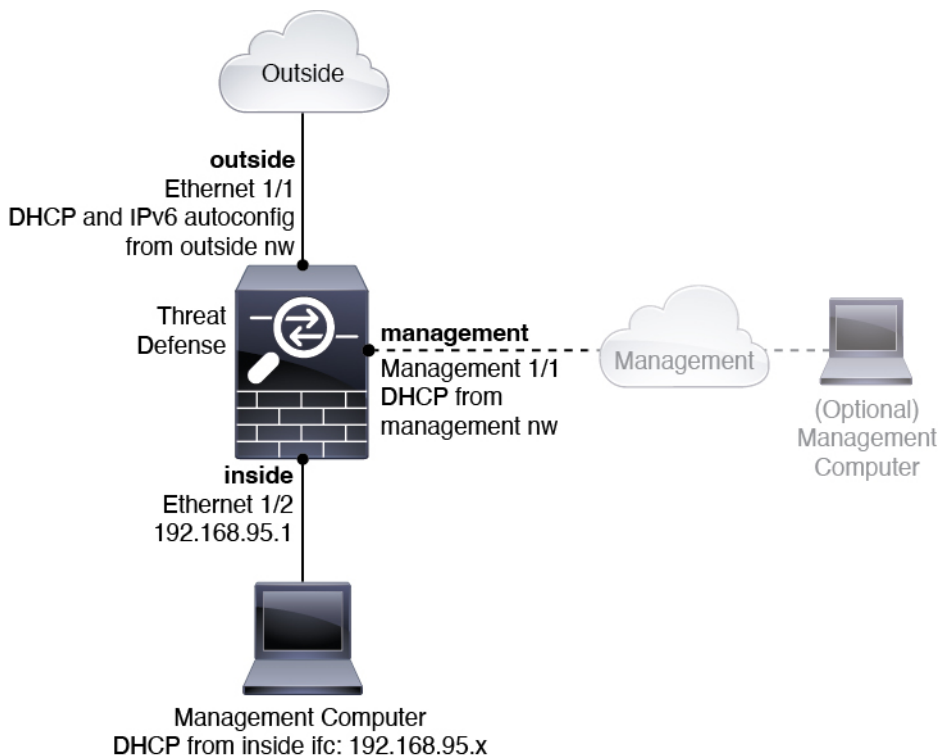
Default Configuration

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

- **inside**—Ethernet 1/2, IP address 192.168.95.1.

- **outside**—Ethernet 1/1, IP address from IPv4 DHCP and IPv6 autoconfiguration

- **inside→outside** traffic flow

- **management**—Management 1/1 (management), IP address from DHCP

Note   The Management 1/1 interface is a special interface separate from data interfaces that is used for management, Smart Licensing, and database updates. (7.4 and later) The Diagnostic interface was merged with the Management interface. (Pre-7.4) 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 Cisco Secure Firewall Device Manager 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**—Obtained from management DHCP. If you do not receive a gateway, then the default route is 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

• **Device Manager access**—All hosts allowed on Management and the inside interface.

• **NAT**—Interface PAT for all traffic from inside to outside

Cable the Firewall

Figure 77: Cabling the Secure Firewall 3100
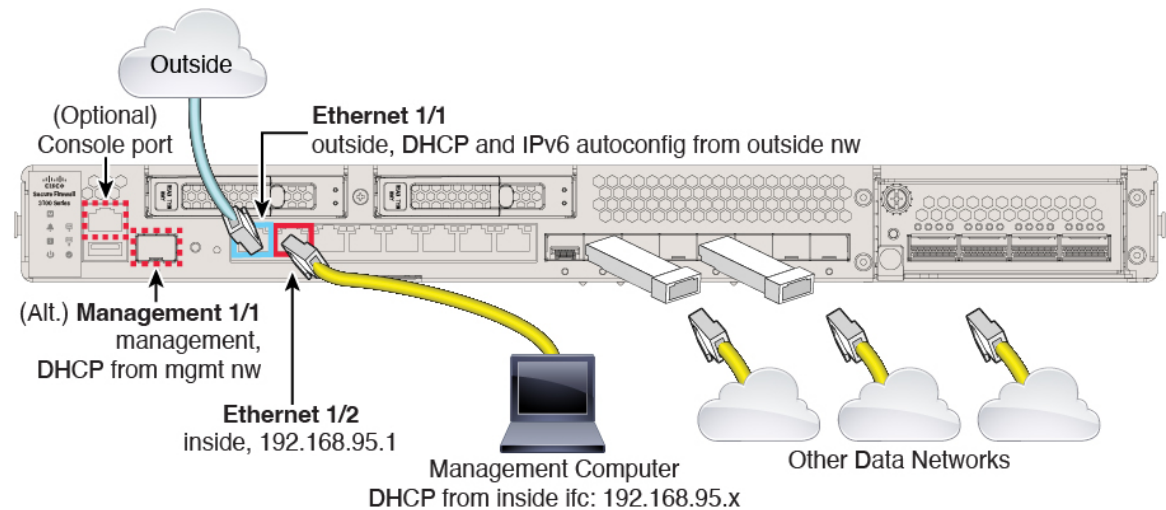
Manage the Secure Firewall 3100 on either Management 1/1 or Ethernet 1/2. The default configuration also configures Ethernet1/1 as outside.

Before you begin

• (Optional) Install an SFP for the Management port—The Management port is a 1/10-Gb SFP port that requires an SFP module.

- (Optional) Obtain a console adapter—The Secure Firewall 3100 ships with a DB-9 to RJ-45 serial cable, so you may need to buy a third party DB-9-to-USB serial cable to make the connection.

Procedure

Step 1   Install the chassis. See the hardware installation guide.

Step 2   Connect your management computer to either of the following interfaces:

- Ethernet 1/2—Connect your management computer directly to Ethernet 1/2 for initial configuration, or connect Ethernet 1/2 to your inside network. Ethernet 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 (see Default Configuration, on page 100).

- Management 1/1—Connect Management 1/1 to your management network, and make sure your management computer is on—or has access to—the management network. Management 1/1 obtains an IP address from a DHCP server on your management network; if you use this interface, you must determine the IP address assigned to the firewall so that you can connect to the IP address from your management computer.

  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 computer to the console port. See (Optional) Check the Software and Install a New Version, on page 103.

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

Step 3   Connect the outside network to the Ethernet1/1 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 4   Connect other networks to the remaining interfaces.

Power on the Firewall

System power is controlled by a rocker power switch located on the rear of the firewall. The power switch is implemented as a soft notification switch that supports graceful shutdown of the system to reduce the risk of system software and data corruption.

Note   The first time you boot up the threat defense, initialization can take approximately 15 to 30 minutes.

Before you begin

It's important that you provide reliable power for your firewall (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 firewall, 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 back of the firewall; if it is solid green, the firewall is powered on.

Figure 78: System and Power LEDs

Step 4 Check the System LED on the back of the firewall; after it is solid green, the system has passed power-on diagnostics.

Note When the switch is toggled from ON to OFF, it may take several seconds for the system to eventually power off. During this time, the Power LED on the front of the chassis blinks green. Do not remove the power until the Power LED is completely off.

(Optional) Check the Software and Install a New Version

To check the software version and, if necessary, install a different version, perform these steps. We recommend that you install your target version before you configure the firewall. Alternatively, you can perform an upgrade after you are up and running, but upgrading, which preserves your configuration, may take longer than using this procedure.

What Version Should I Run?

Cisco recommends running a Gold Star release indicated by a gold star next to the release number on the software download page. You can also refer to the release strategy described in https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html; for example, this bulletin describes short-term release numbering (with the latest features), long-term release numbering (maintenance releases and patches for a longer period of time), or extra long-term release numbering (maintenance releases and patches for the longest period of time, for government certification).

Procedure

Step 1   Connect to the console port. See Access the Threat Defense and the FXOS CLI, on page 118 for more information.

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

You connect to the FXOS CLI. The first time you log in, you are prompted to change the password. This password is also used for the threat defense login for SSH.

Note   If the password was already changed, and you do not know it, you must perform a factory reset to reset the password to the default. See the FXOS troubleshooting guide for the factory reset procedure.

Example:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Step 2   At the FXOS CLI, show the running version.

scope ssa

show app-instance

Example:

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name     Slot ID     Admin State      Operational State     Running Version Startup
 Version Cluster Oper State
-------------------- ---------- --------------- -------------------- ---------------
--------------- -----------------
ftd               1          Enabled       Online            7.6.0.65      7.6.0.65
        Not Applicable
```

Step 3   If you want to install a new version, perform these steps.

a) If you need to set a static IP address for the Management interface, see (Optional) Change Management Network Settings at the CLI, on page 105. By default, the Management interface uses DHCP.

You will need to download the new image from a server accessible from the Management interface.

b) Perform the reimage procedure in the FXOS troubleshooting guide.

After the firewall reboots, you connect to the FXOS CLI again.

c) At the FXOS CLI, you are prompted to set the admin password again.

(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 Cisco Secure Firewall Threat Defense Command Reference.

Procedure

Step 1 Connect to the threat defense console port. See Access the Threat Defense and the FXOS CLI, on page 118 for more information.

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

You connect to the FXOS CLI. The first time you log in, you are prompted to change the password. This password is also used for the threat defense login for SSH.

Note If the password was already changed, and you do not know it, you must perform a factory reset to reset the password to the default. See the FXOS troubleshooting guide for the factory reset procedure.

Example:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Step 2 Connect to the threat defense CLI.

connect ftd

Example:

```
firepower# connect ftd
>
```

Step 3   The first time you log into the threat defense, you are prompted to accept the End User License Agreement (EULA). 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 device manager (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 the device manager 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 device manager. A **no** answer means you intend to use the on-premises or cloud-delivered management center 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 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 4   Log into the device manager on the new Management IP address.

Log Into the Device Manager

Log into the device manager to configure your threat defense.

Procedure

Step 1   Enter the following URL in your browser.

- Inside (Ethernet 1/2)—**https://192.168.95.1**.

- 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.

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

What to do next

- Run through the device manager setup wizard; see

Complete the Initial Configuration

Use the setup wizard when you first log into the device manager 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 (Ethernet1/1) and an inside interface (Ethernet1/2).

- 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 any initial setup at the CLI, 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 the 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 .

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 .

- You can also choose to configure the device using the device manager; see .

Configure Licensing

The threat defense 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

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:

- **Essentials**—(Required) Essentials license.

- **IPS**—Security Intelligence and Next-Generation IPS

- **Malware Defense**—Malware defense

- **URL Filtering**—URL Filtering

- **Cisco Secure Client**—Secure Client Advantage, Secure Client Premier, or Secure Client VPN Only

- **Carrier**—Diameter, GTP/GPRS, M3UA, SCTP

Before you begin

- Have an 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 an 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 **Search All** field on the Cisco Commerce Workspace.

Figure 79: License Search
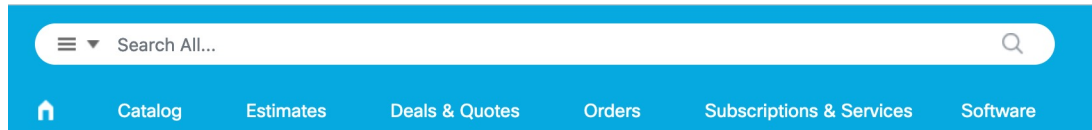
Choose **Products & Services** from the results.

Figure 80: Results

Search for the following license PIDs:

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

- Essentials:

  - *Included automatically*

- IPS, Malware Defense, and URL license combination:

  - L-FPR3110T-TMC=

  - L-FPR3120T-TMC=

  - L-FPR3130T-TMC=

  - L-FPR3140T-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-FPR3110T-TMC-1Y

  - L-FPR3110T-TMC-3Y

  - L-FPR3110T-TMC-5Y

  - L-FPR3120T-TMC-1Y

  - L-FPR3120T-TMC-3Y

  - L-FPR3120T-TMC-5Y

  - L-FPR3130T-TMC-1Y

  - L-FPR3130T-TMC-3Y

  - L-FPR3130T-TMC-5Y

    • L-FPR3140T-TMC-1Y

    • L-FPR3140T-TMC-3Y

    • L-FPR3140T-TMC-5Y

  • Carrier license:

    • L-FPR3K-FTD-CAR=

  • Cisco Secure Client—See the Cisco Secure Client 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**.

Cisco Software Central > **Smart Software Licensing**

Smart Software Licensing

Alerts   **Inventory**   Convert to Smart Licensing

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

Product Instance Registration Tokens

The registration tokens below can be used to register new product instances t

New Token...

Token	Expiration Date	Uses
OWFlNTZiYTgtY2Ew… ⬈	2024-May-18 17:41:53 (in 30 days)	0 of 10
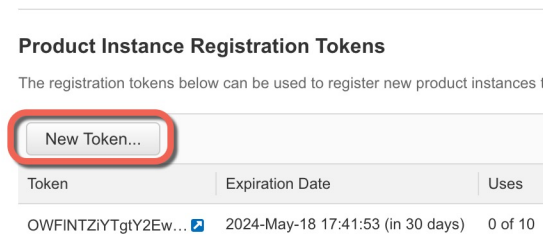
c) On the **Create Registration Token** dialog box enter the following settings, and then click **Create Token**:

Create Registration Token

This will create a token that is used to register product instances, so that they can use licenses from this virtual account.Once it's created, go to the Smart Licensing configuration for your products and enter the token, to register them with this virtual account.

Virtual Account:

Description: Description

* Expire After: 365   Days

                    Between 1 - 365, 30 days recommended

Max. Number of Uses:

                    The token will be expired when either the expiration or the maximum uses is reached

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

Create Token   Cancel

  • **Description**

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

- **Max. Number of Uses**

- **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. 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 threat defense.

Figure 81: View Token

Figure 82: Copy Token
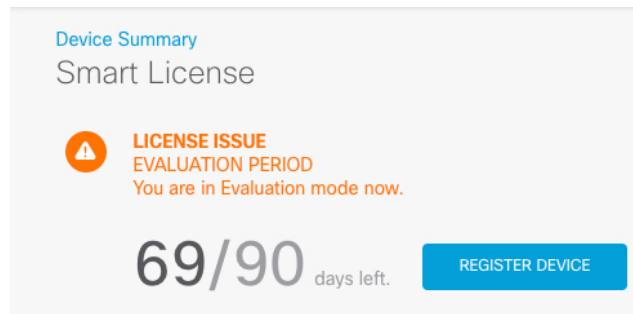
Step 3 In the device manager, click **Device**, and then in the **Smart License** summary, click **View Configuration**.

You see the **Smart License** page.

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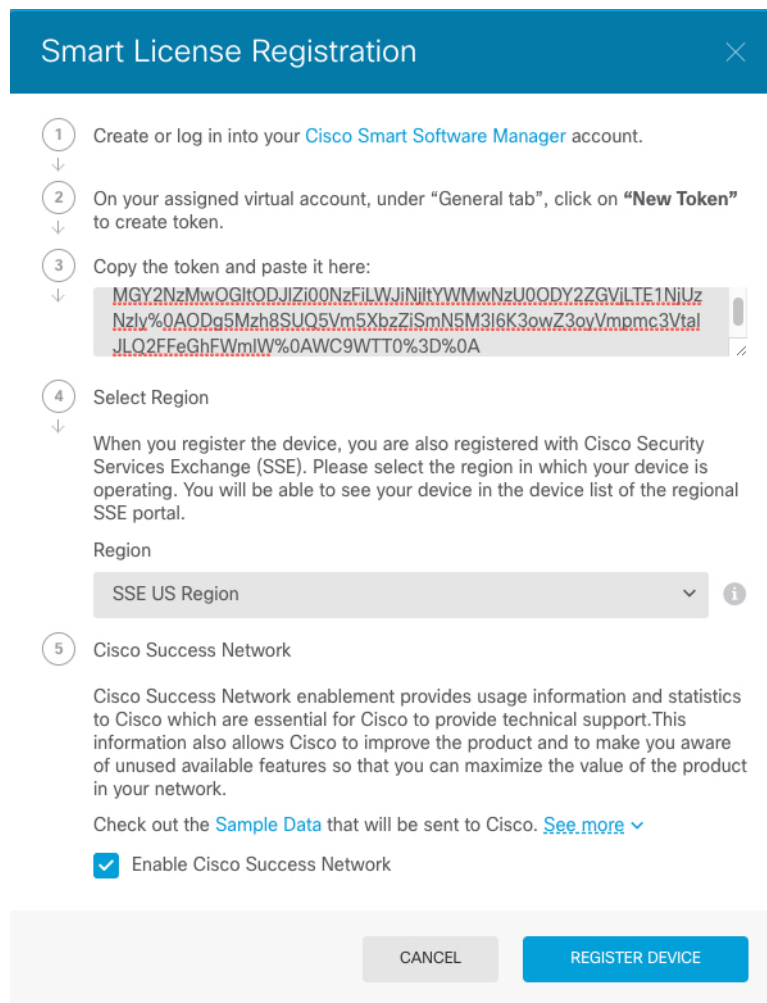
Then follow the instructions on the **Smart License Registration** dialog box to paste in your token:

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 **Cisco Secure Client** license, select the type of license you want to use: **Advantage**, **Premier**, **VPN Only**, or **Premier and Advantage**.

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.
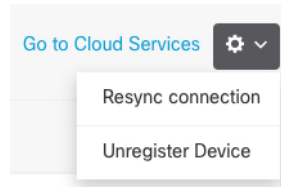
Configure the Firewall in the Device Manager

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   To create 4 x 10-Gb breakout interfaces from a 40-Gb interface (available on some models), choose **Device**, and then click the link in the **Interfaces** summary. Then click the breakout icon for the interface.

If you already used the 40-Gb interface in your configuration, you will have to remove the configuration before you can proceed with the breakout.

Step 2   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 83: Edit Interface

Step 3   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 84: Security Zone Object

Add Security Zone

Name

dmz-zone

Description

Interfaces

+

dmz

Step 4   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 85: DHCP Server

Add Server

Enabled DHCP Server

Interface

inside2

Address Pool

192.168.4.50-192.168.4.240

e.g. 192.168.45.46-192.168.45.254

Step 5   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 86: Default Route

Step 6   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 87: Access Control Policy
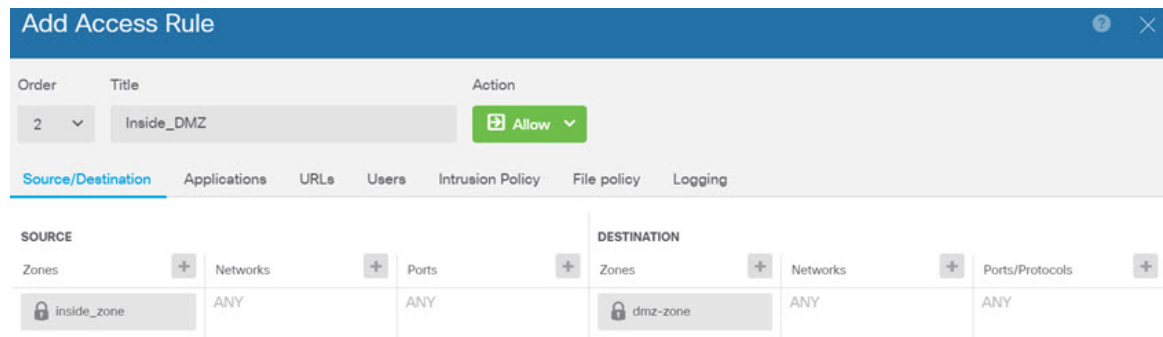
Step 7   Choose **Device**, then click **View Configuration** in the **Updates** group and configure the update schedules for the system databases.

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 8   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 Threat Defense and the FXOS 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 also access the FXOS CLI for troubleshooting purposes.

Note You can alternatively SSH to the Management interface of the threat defense device. Unlike a console session, the SSH session defaults to the threat defense CLI, from which you can connect to the FXOS CLI using the **connect fxos** command. You can later 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. This procedure describes console port access, which defaults to the FXOS CLI.

Procedure

Step 1 To log into the CLI, connect your management computer to the console port. The Secure Firewall 3100 ships with a DB-9 to RJ-45 serial cable, so you may need to buy a third party DB-9-to-USB serial cable to make the connection. Be sure to install any necessary USB serial drivers for your operating system. The console port defaults to the FXOS CLI. Use the following serial settings:

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

You connect to the FXOS CLI. Log in to the CLI using the **admin** username and the password you set at initial setup (the default is **Admin123**).

Example:

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

Step 2 Access the threat defense CLI.

connect ftd

Example:

```
firepower# connect ftd
>
```

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

Step 3 To exit the threat defense CLI, enter the **exit** or **logout** command.

This command returns you to the FXOS CLI prompt. For information on the commands available in the FXOS CLI, enter **?**.

Example:

```
> exit
firepower#
```

Power Off the Firewall

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 firewall system.

You can power off the firewall using device manager, or you can use the FXOS CLI.

Power Off the Firewall Using the Device Manager

Shut down your system properly using the device manager.

Procedure

Step 1 Use the device manager to shut down the firewall.

  a) Click **Device**, then click the **System Settings** > **Reboot/Shutdown** link.
  b) Click **Shut Down**.

Step 2 If you have a console connection to the firewall, monitor the system prompts as the firewall shuts down. You will see the following prompt:

```
System is stopped.
It is safe to power off now.

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

If you do not have a console connection, wait approximately 3 minutes to ensure the system has shut down.

Step 3 You can now turn off the power switch and unplug the power to physically remove power from the chassis if necessary.

Power Off the Firewall at the CLI

You can use the FXOS CLI to safely shut down the system and power off the firewall. You access the CLI by connecting to the console port; see Access the Threat Defense and the FXOS CLI, on page 118.

Procedure

Step 1 In the FXOS CLI, connect to local-mgmt:

firepower # **connect local-mgmt**

Step 2   Issue the **shutdown** command:

firepower(local-mgmt) # **shutdown**

Example:

```
firepower(local-mgmt)# shutdown
This command will shutdown the system.   Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense......ok
```

Step 3   Monitor the system prompts as the firewall shuts down. You will see the following prompt:

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

Step 4   You can now turn off the power switch and unplug the power to physically remove power from the chassis if necessary.

What's Next?

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

For information related to using the device manager, see Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager.

Threat Defense Deployment with CDO

Is This Chapter for You?

To see all available applications and managers, see Which Application and Manager is Right for You?, on page 1. This chapter applies to the threat defense using Cisco Defense Orchestrator (CDO)'s cloud-delivered Firewall Management Center.

Note CDO supports threat defense 7.2 and later.

About the Firewall

The hardware can run either threat defense software or ASA software. Switching between threat defense and ASA requires you to reimage the device. You should also reimage if you need a different software version than is currently installed. See Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.

The firewall runs an underlying operating system called the Secure Firewall eXtensible Operating System (FXOS). The firewall does not support the FXOS Secure Firewall chassis manager; only a limited CLI is supported for troubleshooting purposes. See the Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 and Secure Firewall 3100/4200 with Firepower Threat Defense for more information.

Privacy Collection Statement—The firewall 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 Threat Defense Management by CDO

About the Cloud-delivered Firewall Management Center

The cloud-delivered Firewall Management Center offers many of the same functions as an on-premises management center and has the same look and feel. When you use CDO as the primary manager, you can use an on-prem management center for analytics only. The on-prem management center does not support policy configuration or upgrading.

CDO Onboarding Methods

Use one of the following methods to onboard a device.

Zero-Touch Provisioning

- Send the threat defense to the remote branch office. Do not configure anything on the device, because zero-touch provisioning may not work with pre-configured devices.

  ✎

  Note   You can preregister the threat defense on CDO using the threat defense serial number before sending the device to the branch office.

- At the branch office, cable and power on the threat defense.

- Finish onboarding the threat defense using CDO.

Manual Provisioning

Use the manual onboarding wizard and CLI registration if you need to perform any pre-configuration or if you are using a manager interface that zero-touch provisioning does not support.

Threat Defense Manager Access Interface

This guide covers **outside** interface access because it is the most likely scenario for remote branch offices. Although manager access occurs on the outside interface, the dedicated Management interface is still relevant. The Management interface is a special interface configured separately from the threat defense data interfaces, and it has its own network settings.

- The Management interface network settings are still used even though you are enabling manager access on a data interface.

- All management traffic continues to be sourced from or destined to the Management interface.

- When you enable manager access on a data interface, the threat defense forwards incoming management traffic over the backplane to the Management interface.

- For outgoing management traffic, the Management interface forwards the traffic over the backplane to the data interface.

Manager access from a data interface has the following limitations:

- You can only enable manager access on a physical, data interface. You cannot use a subinterface or EtherChannel, nor can you create a subinterface on the manager access interface. You can also use the management center to enable manager access on a single secondary interface for redundancy.

- This interface cannot be management-only.

- Routed firewall mode only, using a routed interface.

- PPPoE is not supported. If your ISP requires PPPoE, you will have to put a router with PPPoE support between the threat defense and the WAN modem.

- The interface must be in the global VRF only.

- SSH is not enabled by default for data interfaces, so you will have to enable SSH later using the management center. Because the Management interface gateway will be changed to be the data interfaces, you also cannot SSH to the Management interface from a remote network unless you add a static route for the Management interface using the **configure network static-routes** command.

- Clustering is not supported. You must use the Management interface in this case.

- High availability is not supported. You must use the Management interface in this case.

End-to-End Tasks: Zero-Touch Provisioning

See the following tasks to deploy the threat defense with CDO using zero-touch provisioning.

Figure 88: End-to-End Procedure: Zero-Touch Provisioning
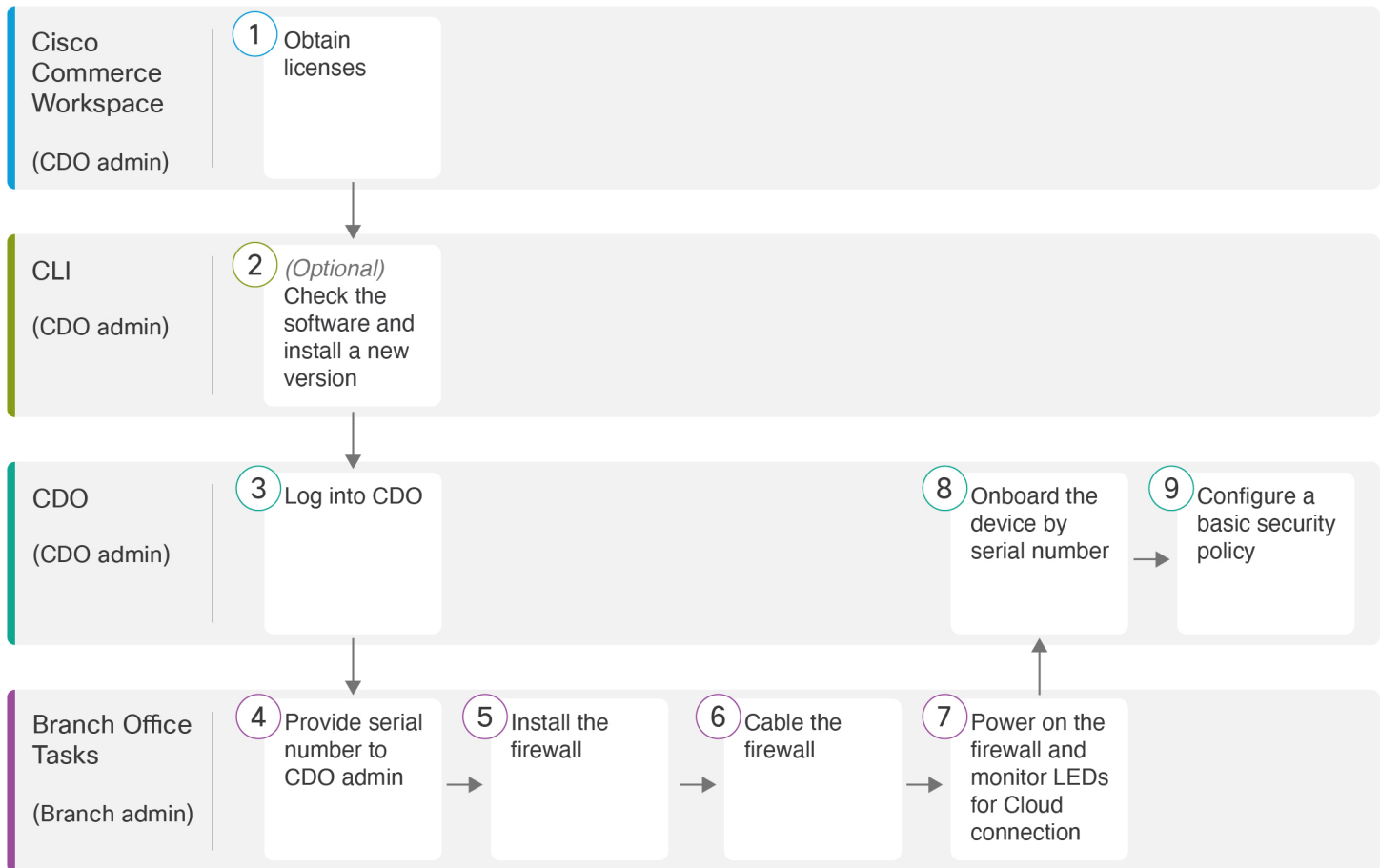
1	Cisco Commerce Workspace (CDO admin)	Obtain Licenses, on page 128.
2	CLI (CDO admin)	(Optional) Check the Software and Install a New Version, on page 130.
3	CDO (CDO admin)	Log Into CDO, on page 132.
4	Branch Office Tasks (Branch admin)	Provide the Firewall Serial Number to the Central Administrator, on page 132.
5	Branch Office Tasks (Branch admin)	Install the firewall. See the hardware installation guide.
6	Branch Office Tasks (Branch admin)	Cable the Firewall, on page 132.

7	Branch Office Tasks (Branch admin)	Power On the Firewall, on page 133.
8	CDO (CDO admin)	Onboard a Device with Zero-Touch Provisioning, on page 135.
9	CDO (CDO admin)	Configure a Basic Security Policy, on page 152.

End-to-End Tasks: Onboarding Wizard

See the following tasks to onboard the threat defense to CDO using the onboarding wizard.

Figure 89: End-to-End Procedure: Onboarding Wizard

1	Cisco Commerce Workspace	Obtain Licenses, on page 128.

2	CLI	(Optional) Check the Software and Install a New Version, on page 130.
3	CDO	Log Into CDO, on page 132.
4	Physical Tasks	Install the firewall. See the hardware installation guide.
5	Physical Tasks	Cable the Firewall, on page 138.
6	Physical Tasks	Power on the Firewall, on page 139.
7	CDO	Onboard a Device with the Onboarding Wizard, on page 140.
8	CLI or Device Manager	• Perform Initial Configuration Using the CLI, on page 143. • Perform Initial Configuration Using the Device Manager, on page 147.
9	CDO	Configure a Basic Security Policy, on page 152.

Central Administrator Pre-Configuration

This section describes how to obtain feature licenses for your firewall; how to install a new software version before you deploy; and how to log into CDO.

Obtain Licenses

All licenses are supplied to the threat defense by CDO. You can optionally purchase the following feature licenses:

- **Essentials**—(Required) Essentials license.

- **IPS**—Security Intelligence and Next-Generation IPS

- **Malware Defense**—Malware defense

- **URL Filtering**—URL Filtering

- **Cisco Secure Client**—Secure Client Advantage, Secure Client Premier, or Secure Client VPN Only

- **Carrier**—Diameter, GTP/GPRS, M3UA, SCTP

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

Before you begin

- Have an 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 an 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 **Search All** field on the Cisco Commerce Workspace.

Figure 90: License Search
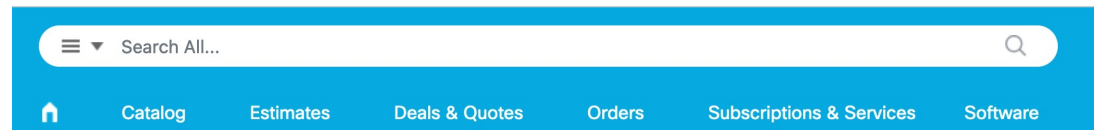
Choose **Products & Services** from the results.

Figure 91: Results

Search for the following license PIDs:

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

• Essentials:

    • *Included automatically*

• IPS, Malware Defense, and URL license combination:

    • L-FPR3110T-TMC=

    • L-FPR3120T-TMC=

    • L-FPR3130T-TMC=

    • L-FPR3140T-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-FPR3110T-TMC-1Y

- L-FPR3110T-TMC-3Y

- L-FPR3110T-TMC-5Y

- L-FPR3120T-TMC-1Y

- L-FPR3120T-TMC-3Y

- L-FPR3120T-TMC-5Y

- L-FPR3130T-TMC-1Y

- L-FPR3130T-TMC-3Y

- L-FPR3130T-TMC-5Y

- L-FPR3140T-TMC-1Y

- L-FPR3140T-TMC-3Y

- L-FPR3140T-TMC-5Y

- Carrier license:

  - L-FPR3K-FTD-CAR=

- Cisco Secure Client—See the Cisco Secure Client Ordering Guide.

Step 2 If you have not already done so, register CDO with the Smart Software Manager.

Registering requires you to generate a registration token in the Smart Software Manager. See the CDO documentation for detailed instructions.

(Optional) Check the Software and Install a New Version

To check the software version and, if necessary, install a different version, perform these steps. We recommend that you install your target version before you configure the firewall. Alternatively, you can perform an upgrade after you are up and running, but upgrading, which preserves your configuration, may take longer than using this procedure.

What Version Should I Run?

Cisco recommends running a Gold Star release indicated by a gold star next to the release number on the software download page. You can also refer to the release strategy described in https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html; for example, this bulletin describes short-term release numbering (with the latest features), long-term release numbering (maintenance releases and patches for a longer period of time), or extra long-term release numbering (maintenance releases and patches for the longest period of time, for government certification).

Procedure

Step 1 Power on the firewall and connect to the console port. See Power on the Firewall, on page 139 and Access the Threat Defense and FXOS CLI, on page 166 for more information.

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

You connect to the FXOS CLI. The first time you log in, you are prompted to change the password. This password is also used for the threat defense login for SSH.

Note If the password was already changed, and you do not know it, you must perform a factory reset to reset the password to the default. See the FXOS troubleshooting guide for the factory reset procedure.

Example:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Step 2 At the FXOS CLI, show the running version.

scope ssa

show app-instance

Example:

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name    Slot ID    Admin State    Operational State    Running Version Startup
 Version Cluster Oper State
------------------- ---------- -------------- -------------------- ---------------
--------------- ------------------
ftd                 1          Enabled        Online               7.6.0.65        7.6.0.65
        Not Applicable
```

Step 3 If you want to install a new version, perform these steps.

a) If you need to set a static IP address for the Management interface, see Perform Initial Configuration Using the CLI, on page 143. By default, the Management interface uses DHCP.

You will need to download the new image from a server accessible from the Management interface.

b) Perform the reimage procedure in the FXOS troubleshooting guide.

After the firewall reboots, you connect to the FXOS CLI again.

    c)   At the FXOS CLI, you are prompted to set the admin password again.

         For zero-touch provisioning, when you onboard the device, for the **Password Reset** area, be sure to choose **No...** because you already set the password.

    d)   Shut down the device. See .

Log Into CDO

For details on creating a CDO tenant and logging in, see the CDO doucmentation: https://docs.defenseorchestrator.com.

Deploy the Firewall With Low-Touch Provisioning

After you receive the threat defense from central headquarters, you only need to cable and power on the firewall so that it has internet access from the outside interface. The central administrator can then complete the configuration.

Provide the Firewall Serial Number to the Central Administrator

Before you rack the firewall or discard the shipping box, record the serial number so you can coordinate with the central adminstrator.

Procedure

Step 1   Unpack the chassis and chassis components.

Take inventory of your firewall and packaging before you connect any cables or power on the firewall. You should also familiarize yourself with the chassis layout, components, and LEDs.

Step 2   Record the firewall's serial number.

The serial number of the firewall can be found on the shipping box. It can also be found on a sticker on a pull-out tab on the front of the firewall.

Step 3   Send the firewall serial number to the CDO network administrator at your IT department/central headquarters.

Your network administrator needs your firewall serial number to facilitate low-touch provisioning, connect to the firewall, and configure it remotely.

Communicate with the CDO administrator to develop an onboarding timeline.

Cable the Firewall

Connect the Secure Firewall 3100 so that it can be managed by CDO.

If you received a firewall at your branch office, and your job is to plug it in to your network, watch this video. The video describes your firewall and the LED sequences on the firewall that indicate the firewall's status. If you need to, you'll be able to confirm the firewall's status with your IT department just by looking at the LEDs.

Figure 92: Cabling the Secure Firewall 3100
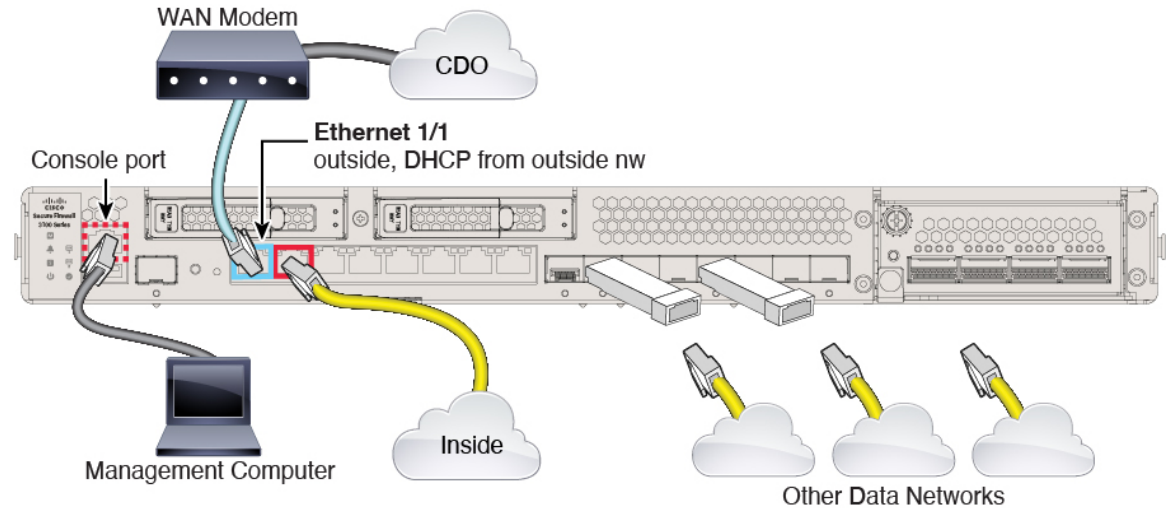
Before you begin

(Optional) Obtain a console adapter—The Secure Firewall 3100 ships with a DB-9 to RJ-45 serial cable, so you may need to buy a third party DB-9-to-USB serial cable to make the connection.

Procedure

Step 1   Install the chassis. See the hardware installation guide.

Step 2   Connect the network cable from the Ethernet 1/1 interface to your wide area network (WAN) modem. Your WAN modem is your branch's connection to the internet and will be your firewall's route to the internet as well.

Step 3   Connect the inside interface (for example, Ethernet 1/2) to your inside switch or router.

     You can choose any interface for inside.

Step 4   Connect other networks to the remaining interfaces.

Step 5   (Optional) Connect the management computer to the console port.

     At the branch office, the console connection is not required for everyday use; however, it may be required for troubleshooting purposes.

Power On the Firewall

System power is controlled by a rocker power switch located on the rear of the firewall. The power switch is implemented as a soft notification switch that supports graceful shutdown of the system to reduce the risk of system software and data corruption.

Note The first time you boot up the threat defense, initialization can take approximately 15 to 30 minutes.

Before you begin

It's important that you provide reliable power for your firewall (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 firewall, 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 back of the firewall; if it is solid green, the firewall is powered on.

Figure 93: Managed, Power, and System LEDs
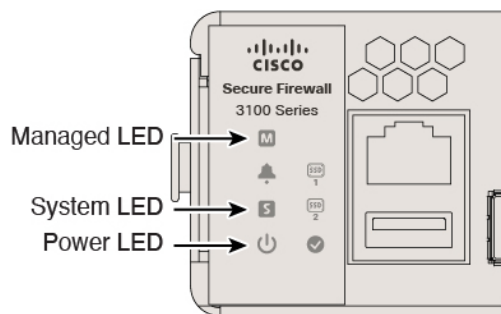
Step 4 Check the System LED on the back of the firewall; after it is solid green, the system has passed power-on diagnostics.

Note When the switch is toggled from ON to OFF, it may take several seconds for the system to eventually power off. During this time, the Power LED on the front of the chassis blinks green. Do not remove the power until the Power LED is completely off.

Step 5 Check the Managed LED on the back of the firewall; when the firewall connects to the Cisco cloud, the Managed LED slowly flashes green.

If there is a problem, the Managed LED flashes amber and green to indicate that the firewall did not reach the Cisco Cloud. If you see this pattern, make sure that your network cable is connected to the Ethernet 1/1 interface and to your WAN modem. If after adjusting the network cable, the firewall does not reach the Cisco cloud after approximately 10 more minutes, call your IT department.

What to do next

- Communicate with your IT department to confirm your onboarding timeline and activities. You should have a communication plan in place with the CDO administrator at your central headquarters.

- After you complete this task, your CDO administrator will be able to configure and manage the firewall remotely. You're done.

Onboard a Device with Zero-Touch Provisioning

Onboard the threat defense using zero-touch provisioning and the device serial number.

Procedure

Step 1   In the CDO navigation pane, click **Inventory**, then click the blue plus button (![+]( )) to **Onboard** a device.

Step 2   Select the **FTD** tile.

Step 3   Under **Management Mode**, be sure **FTD** is selected.

At any point after selecting **FTD** as the management mode, you can click **Manage Smart License** to enroll in or modify the existing smart licenses available for your device. See Obtain Licenses, on page 128 to see which licenses are available.

Step 4   Select **Use Serial Number** as the onboarding method.

Figure 94: Use Serial Number
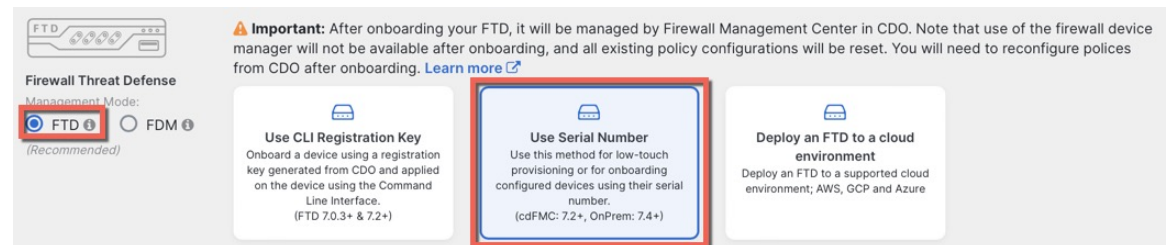
Step 5   In **Select FMC**, choose the **Cloud-Delivered FMC** > **Firewall Management Center** from the list, and click **Next**.

Figure 95: Select FMC

Step 6   In the **Connection** area, enter the **Device Serial Number** and the **Device Name** and then click **Next**.

Figure 96: Connection

Step 7   In **Password Reset**, click **Yes...**. Enter a new password and confirm the new password for the device, then click **Next**.

For low-touch provisioning, the device must be brand new or has been reimaged.

Note   If you did log into the device and reset the password, and you did not change the configuration in a way that would disable low-touch provisioning, then you should choose the **No...** option. There are a number of configurations that disable low-touch provisioning, so we don't recommend logging into the device unless you need to, for example, to perform a reimage.

Figure 97: Password Reset

Step 8   For the **Policy Assignment**, use the drop-down menu to choose an access control policy for the device. If you have no policies configured, choose the **Default Access Control Policy**.

Figure 98: Policy Assignment

Step 9   For the **Subscription License**, check each of the feature licenses you want to enable. Click **Next**.

Figure 99: Subscription License

Step 10   (Optional) Add labels to your device to help sort and filter the **Inventory** page. Enter a label and select the

blue plus button ( ). Labels are applied to the device after it's onboarded to CDO.

Figure 100: Done

What to do next

From the **Inventory** page, select the device you just onboarded and select any of the option listed under the **Management** pane located to the right.

Deploy the Firewall With the Onboarding Wizard

This section describes how to configure the firewall for onboarding using the CDO onboarding wizard.

Cable the Firewall

Connect the Secure Firewall 3100 so that it can be managed by CDO.

Figure 101: Cabling the Secure Firewall 3100
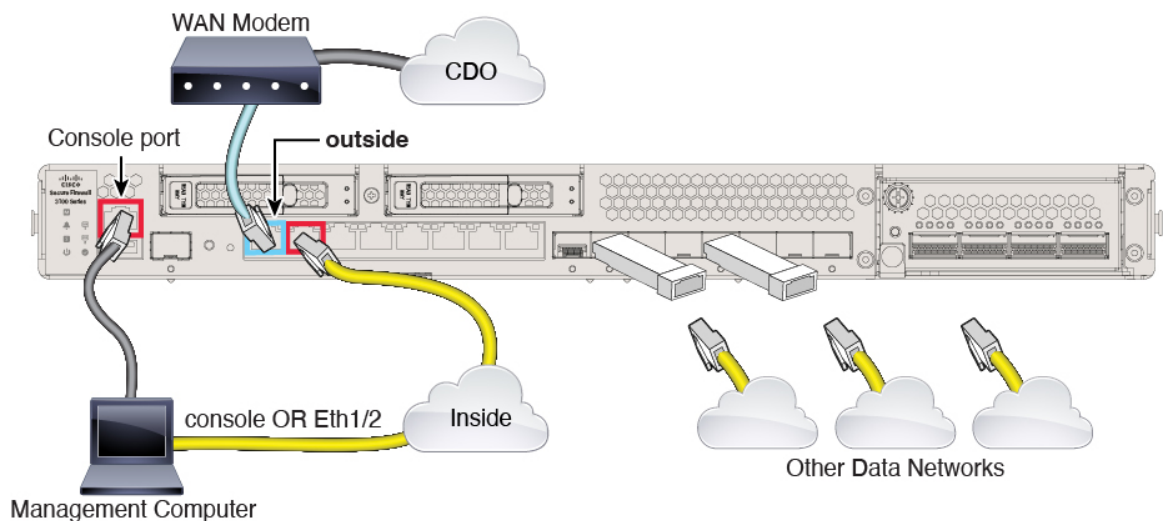
Before you begin

Obtain a console adapter—The Secure Firewall 3100 ships with a DB-9 to RJ-45 serial cable, so you may need to buy a third party DB-9-to-USB serial cable to make the connection.

Procedure

Step 1 Install the chassis. See the hardware installation guide.

Step 2 Connect the outside interface (for example, Ethernet 1/1) to your outside router.

Step 3 Connect the inside interface (for example, Ethernet 1/2) to your inside switch or router.

Step 4 Connect other networks to the remaining interfaces.

Step 5 Connect the management computer to the console port or the Ethernet 1/2 interface.

If you perform intial setup using the CLI, you will need to connect to the console port. The console port may also be required for troubleshooting purposes. If you perform initial setup using the device manager, connect to the Ethernet 1/2 interface.

Power on the Firewall

System power is controlled by a rocker power switch located on the rear of the firewall. The power switch is implemented as a soft notification switch that supports graceful shutdown of the system to reduce the risk of system software and data corruption.

Note The first time you boot up the threat defense, initialization can take approximately 15 to 30 minutes.

Before you begin

It's important that you provide reliable power for your firewall (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 firewall, 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 back of the firewall; if it is solid green, the firewall is powered on.

Figure 102: System and Power LEDs
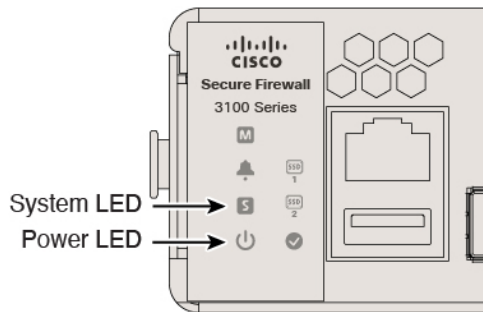
Step 4   Check the System LED on the back of the firewall; after it is solid green, the system has passed power-on diagnostics.

> **Note**   When the switch is toggled from ON to OFF, it may take several seconds for the system to eventually power off. During this time, the Power LED on the front of the chassis blinks green. Do not remove the power until the Power LED is completely off.

Onboard a Device with the Onboarding Wizard

Onboard the threat defense using CDO's onboarding wizard using a CLI registration key.

Procedure

Step 1   In the CDO navigation pane, click **Inventory**, then click the blue plus button ( ) to **Onboard** a device.

Step 2   Click the **FTD** tile.

Step 3   Under **Management Mode**, be sure **FTD** is selected.

At any point after selecting **FTD** as the management mode, you can click **Manage Smart License** to enroll in or modify the existing smart licenses available for your device. See Obtain Licenses, on page 128 to see which licenses are available.

Step 4   Select **Use CLI Registration Key** as the onboarding method.

Figure 103: Use CLI Registration Key
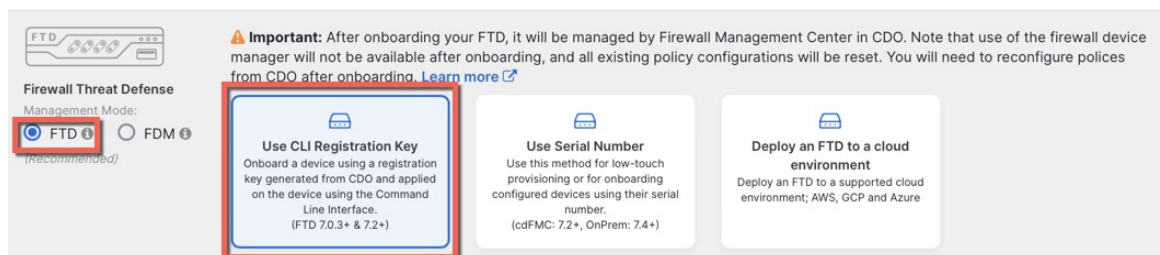
Step 5   Enter the **Device Name** and click **Next**.

Figure 104: Device Name

Step 6   For the **Policy Assignment**, use the drop-down menu to choose an access control policy for the device. If you have no policies configured, choose the **Default Access Control Policy**.

Figure 105: Access Control Policy

Step 7   For the **Subscription License**, click the **Physical FTD Device** radio button, and then check each of the feature licenses you want to enable. Click **Next**.

Figure 106: Subscription License

Step 8   For the **CLI Registration Key**, CDO generates a command with the registration key and other parameters. You must copy this command and use it in the intial configuration of the threat defense.

Figure 107: CLI Registration Key
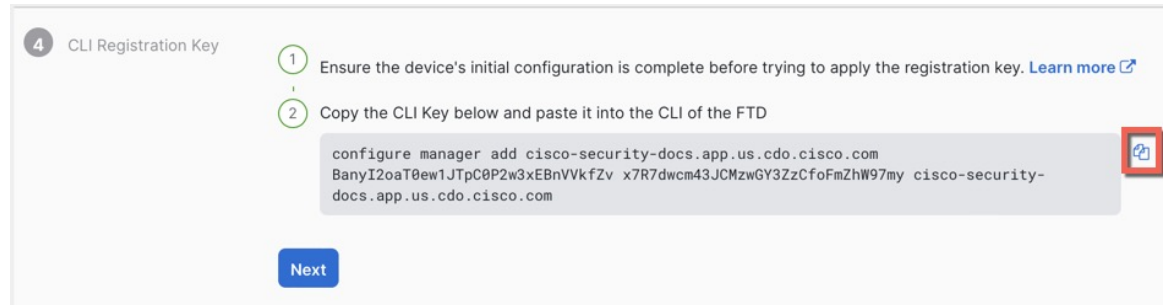
configure manager add *cdo_hostname registration_key nat_id display_name*

Complete initial configuration at the CLI or using the device manager:

- Perform Initial Configuration Using the CLI, on page 143—Copy this command at the threat defense CLI after you complete the startup script.

- Perform Initial Configuration Using the Device Manager, on page 147—Copy the *cdo_hostname*, *registration_key*, and *nat_id* parts of the command into the **Management Center/CDO Hostname/IP Address**, **Management Center/CDO Registration Key**, and **NAT ID** fields.

Example:

Sample command for CLI setup:

```
configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
```

Sample command components for GUI setup:

Figure 108: configure manager add command components
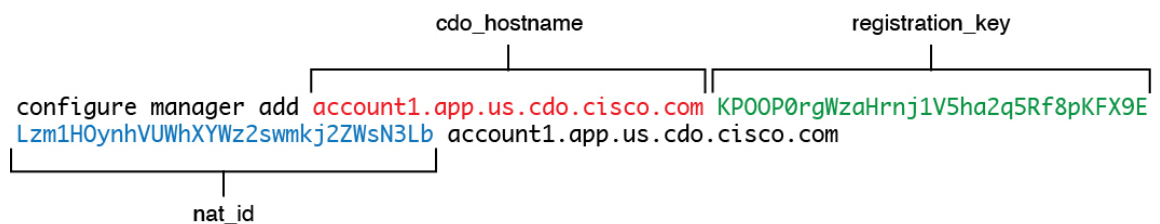
Step 9   Click **Next** in the onboarding wizard to start registering the device.

Step 10   (Optional) Add labels to your device to help sort and filter the **Inventory** page. Enter a label and select the blue plus button ( ). Labels are applied to the device after it's onboarded to CDO.

Figure 109: Done
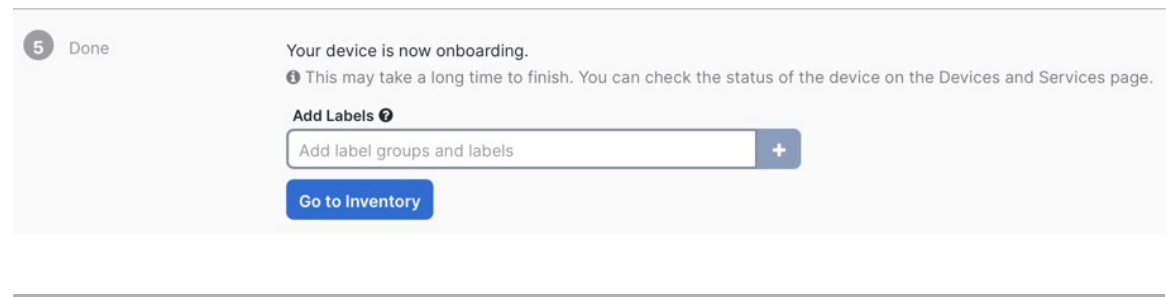
What to do next

From the **Inventory** page, select the device you just onboarded and select any of the option listed under the **Management** pane located to the right.

Perform Initial Configuration

Perfom initial configuration of the threat defense using the CLI or using the device manager.

Perform Initial Configuration Using the CLI

Connect to the threat defense CLI to perform initial setup. When you use the CLI for initial configuration, only the Management interface and manager access interface settings are retained.When you perform initial setup using the device manager, *all* interface configuration completed in the device manager is retained when you switch to CDO for management, in addition to the Management interface and manager access interface settings. Note that other default configuration settings, such as the access control policy, are not retained.

Procedure

Step 1   Connect to the threat defense CLI on the console port.

The console port connects to the FXOS CLI.

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

The first time you log in to FXOS, you are prompted to change the password. This password is also used for the threat defense login for SSH.

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

Example:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
```

```
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Step 3   Connect to the threat defense CLI.

connect ftd

Example:

```
firepower# connect ftd
>
```

Step 4   The first time you log in to the threat defense, you are prompted to accept the End User License Agreement (EULA). You are then presented with the CLI setup script for the Management interface settings.

The Management interface settings are used even though you are enabling manager access on a data interface.

Note   You cannot repeat the CLI setup wizard 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 Cisco Secure Firewall Threat Defense Command Reference.

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

See the following guidelines:

- **Do you want to configure IPv4?** and/or **Do you want to configure IPv6?**—Enter **y** for at least one of these types of addresses. Although you do not plan to use the Management interface, you must set an IP address, for example, a private address.

- **Configure IPv4 via DHCP or manually?** and/or **Configure IPv6 via DHCP, router, or manually?**—Choose **manual**. You cannot configure a data interface for management if the management interface is set to DHCP, because the default route, which must be **data-interfaces** (see the next bullet), might be overwritten with one received from the DHCP server.

- **Enter the IPv4 default gateway for the management interface** and/or **Enter the IPv6 gateway for the management interface**—Set the gateway to be **data-interfaces**. This setting forwards management traffic over the backplane so it can be routed through the manager access data interface.

- **Manage the device locally?**—Enter **no** to use CDO. A **yes** answer means you will use the device manager instead.

- **Configure firewall mode?**—Enter **routed**. Outside manager access is only supported in routed firewall mode.

Example:

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

System initialization in progress.  Please stand by.
You must configure the network to continue.
Configure at least one of IPv4 or IPv6 unless managing via data interfaces.
```

```
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [y]: n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.61]: 10.89.5.17
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]:
Enter a fully qualified hostname for this system [firepower]: 1010-3
Enter a comma-separated list of DNS servers or 'none'
[208.67.222.222,208.67.220.220,2620:119:35::35]:
Enter a comma-separated list of search domains or 'none' []: cisco.com
If your networking information has changed, you will need to reconnect.
Disabling IPv6 configuration: management0
Setting DNS servers: 208.67.222.222,208.67.220.220,2620:119:35::35
Setting DNS domains:cisco.com
Setting hostname as 1010-3
Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: data on management0
Updating routing tables, please wait...
All configurations applied to the system. Took 3 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
DHCP server is already disabled
DHCP Server Disabled
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...


Device is in OffBox mode - disabling/removing port 443 from iptables.
Update policy deployment information
    - add device configuration
    - add network discovery
    - add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required.  In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>
```

Step 5 Configure the outside interface for manager access.

configure network management-data-interface

You are then prompted to configure basic network settings for the outside interface. See the following details for using this command:

- The Management interface cannot use DHCP if you want to use a data interface for management. If you did not set the IP address manually during initial setup, you can set it now using the **configure network**

{**ipv4** | **ipv6**} **manual** command. If you did not already set the Management interface gateway to **data-interfaces**, this command will set it now.

- When you add the threat defense to CDO, CDO discovers and maintains the interface configuration, including the following settings: interface name and IP address, static route to the gateway, DNS servers, and DDNS server. For more information about the DNS server configuration, see below. In CDO, you can later make changes to the manager access interface configuration, but make sure you don't make changes that can prevent the threat defense or CDO from re-establishing the management connection. If the management connection is disrupted, the threat defense includes the **configure policy rollback** command to restore the previous deployment.

- If you configure a DDNS server update URL, the threat defense automatically adds certificates for all of the major CAs from the Cisco Trusted Root CA bundle so that the threat defense can validate the DDNS server certificate for the HTTPS connection. The threat defense supports any DDNS server that uses the DynDNS Remote API specification (https://help.dyn.com/remote-access-api/).

- This command sets the *data* interface DNS server. The Management DNS server that you set with the setup script (or using the **configure network dns servers** command) is used for management traffic. The data DNS server is used for DDNS (if configured) or for security policies applied to this interface.

  On CDO, the data interface DNS servers are configured in the Platform Settings policy that you assign to this threat defense. When you add the threat defense to CDO, the local setting is maintained, and the DNS servers are *not* added to a Platform Settings policy. However, if you later assign a Platform Settings policy to the threat defense that includes a DNS configuration, then that configuration will overwrite the local setting. We suggest that you actively configure the DNS Platform Settings to match this setting to bring CDO and the threat defense into sync.

  Also, local DNS servers are only retained by CDO if the DNS servers were discovered at initial registration. For example, if you registered the device using the Management interface, but then later configure a data interface using the **configure network management-data-interface** command, then you must manually configure all of these settings in CDO, including the DNS servers, to match the threat defense configuration.

- You can change the management interface after you register the threat defense to CDO, to either the Management interface or another data interface.

- The FQDN that you set in the setup wizard will be used for this interface.

- You can clear the entire device configuration as part of the command; you might use this option in a recovery scenario, but we do not suggest you use it for initial setup or normal operation.

- To disable data managemement, enter the **configure network management-data-interface disable** command.

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://deanwinchester:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.
```

```
Setting IPv4 network configuration.
Network settings changed.

>
```

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Step 6   Identify the CDO that will manage this threat defense using the **configure manager add** command that CDO generated. See to generate the command.

Example:

```
> configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
Manager successfully configured.
```

Perform Initial Configuration Using the Device Manager

When you use the device manager for initial setup, the following interfaces are preconfigured in addition to the Management interface and manager access settings:

- Ethernet 1/1—"outside", IP address from DHCP, IPv6 autoconfiguration

- Ethernet 1/2— "inside", 192.168.95.1/24

- Default route—Obtained through DHCP on the outside interface

Note that other settings, such as the DHCP server on inside, access control policy, or security zones, are not configured.

If you perform additional interface-specific configuration within device manager before onboarding to CDO, then that configuration is preserved.

When you use the CLI, only the Management interface and manager access settings are retained (for example, the default inside interface configuration is not retained).

Procedure

Step 1   Connect your management computer to the Ethernet1/2 interface.

Step 2   Log in to the device manager.

   a) Enter the following URL in your browser: **https://192.168.95.1**

   b) Log in with the username **admin**, and the default password **Admin123**.

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

Step 3   Use the setup wizard when you first log into the device manager to complete the initial configuration. You can optionally skip the setup wizard by clicking **Skip device setup** at the bottom of the page.

   After you complete the setup wizard, in addition to the default configuraton for the inside interface (Ethernet1/2), you will have configuration for an outside (Ethernet1/1) interface that will be maintained when you switch to CDO management.

   a) Configure the following options for the outside and management interfaces and click **Next**.

   1. **Outside Interface Address**—This interface is typically the internet gateway, and might be used as your manager access interface. You cannot select an alternative outside interface during initial device setup. The first data interface is the default outside interface.

   If you want to use a different interface from outside (or inside) for manager access, you will have to configure it manually after completing the setup wizard.

   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.

   2. **Management Interface**

   You will not see Management Interface settings if you performed intial setup at the CLI.

   The Management interface settings are used even though you are enabling the manager access on a data interface. For example, the management traffic that is routed over the backplane through the data interface will resolve FQDNs using the Management interface DNS servers, and not the data interface DNS servers.

   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.

   b) Configure the **Time Setting (NTP)** and click **Next**.

   1. **Time Zone**—Select the time zone for the system.

   2. **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.

c) Select **Start 90 day evaluation period without registration**.

Do not register the threat defense with the Smart Software Manager; all licensing is performed in CDO.

d) Click **Finish**.

e) You are prompted to choose **Cloud Management** or **Standalone**. For the CDO cloud-delivered management center, choose **Standalone**, and then **Got It**.

The **Cloud Management** option is for legacy CDO/FDM functionality.

Step 4   (Might be required) Configure the Management interface. See the Management interface on **Device** > **Interfaces**.

The Management interface must have the gateway set to data interfaces. By default, the Management interface receives an IP address and gateway from DHCP. If you do not receive a gateway from DHCP (for example, you did not connect this interface to a network), then the gateway will default to data interfaces, and you do not need to configure anything. If you did receive a gateway from DHCP, then you need to instead configure this interface with a static IP address and set the gateway to data interfaces.

Step 5   If you want to configure additional interfaces, including an interface other than outside or inside that you want to use for the manager access, choose **Device**, and then click the link in the **Interfaces** summary.

See Configure the Firewall in the Device Manager, on page 115 for more information about configuring interfaces in the device manager. Other device manager configuration will not be retained when you register the device to CDO.

Step 6   Choose **Device** > **System Settings** > **Central Management**, and click **Proceed** to set up the management center management.

Step 7   Configure the **Management Center/CDO Details**.

Figure 110: Management Center/CDO Details

a) For **Do you know the Management Center/CDO hostname or IP address**, click **Yes**.

CDO generates the **configure manager add** command. See Onboard a Device with the Onboarding Wizard, on page 140 to generate the command.

configure manager add *cdo_hostname registration_key nat_id display_name*

Example:

Figure 111: configure manager add command components
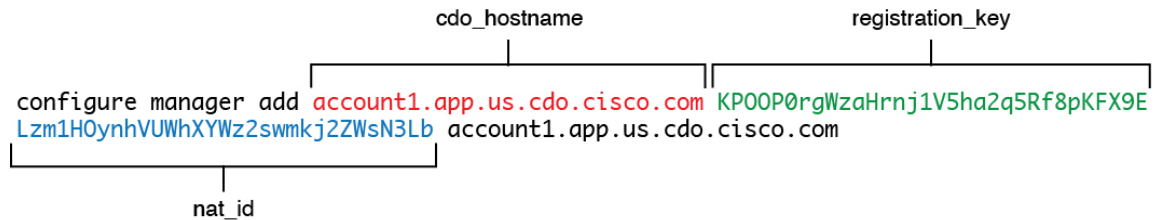
b) Copy the *cdo_hostname*, *registration_key*, and *nat_id* parts of the command into the **Management Center/CDO Hostname/IP Address**, **Management Center/CDO Registration Key**, and **NAT ID** fields.

Step 8   Configure the **Connectivity Configuration**.

a) Specify the **FTD Hostname**.

This FQDN will be used for the outside interface, or whichever interface you choose for the **Management Center/CDO Access Interface**.

b) Specify the **DNS Server Group**.

Choose an existing group, or create a new one. The default DNS group is called **CiscoUmbrellaDNSServerGroup**, which includes the OpenDNS servers.

This setting sets the *data* interface DNS server. The Management DNS server that you set with the setup wizard is used for management traffic. The data DNS server is used for DDNS (if configured) or for security policies applied to this interface. You are likley to choose the same DNS server group that you used for Management, because both management and data traffic reach the DNS server through the outside interface.

On CDO, the data interface DNS servers are configured in the Platform Settings policy that you assign to this threat defense. When you add the threat defense to CDO, the local setting is maintained, and the DNS servers are *not* added to a Platform Settings policy. However, if you later assign a Platform Settings policy to the threat defense that includes a DNS configuration, then that configuration will overwrite the local setting. We suggest that you actively configure the DNS Platform Settings to match this setting to bring CDO and the threat defense into sync.

Also, local DNS servers are only retained by CDO if the DNS servers were discovered at initial registration.

c) For the **Management Center/CDO Access Interface**, choose **outside**.

You can choose any configured interface, but this guide assumes you are using outside.

Step 9   If you chose a different data interface from outside, then add a default route.

You will see a message telling you to check that you have a default route through the interface. If you chose outside, you already configured this route as part of the setup wizard. If you chose a different interface, then you need to manually configure a default route before you connect to CDO. See Configure the Firewall in the Device Manager, on page 115 for more information about configuring static routes in the device manager.

Step 10   Click **Add a Dynamic DNS (DDNS) method**.

DDNS ensures CDO can reach the threat defense at its Fully-Qualified Domain Name (FQDN) if the threat defense's IP address changes. See **Device** > **System Settings** > **DDNS Service** to configure DDNS.

If you configure DDNS before you add the threat defense to CDO, the threat defense automatically adds certificates for all of the major CAs from the Cisco Trusted Root CA bundle so that the threat defense can validate the DDNS server certificate for the HTTPS connection. The threat defense supports any DDNS server that uses the DynDNS Remote API specification (https://help.dyn.com/remote-access-api/).

Step 11 Click **Connect**. The **Registration Status** dialog box shows the current status of the switch to CDO. After the **Saving Management Center/CDO Registration Settings** step, go to CDO, and add the firewall.

If you want to cancel the switch to CDO, click **Cancel Registration**. Otherwise, do not close the device manager browser window until after the **Saving Management Center/CDO Registration Settings** step. If you do, the process will be paused, and will only resume when you reconnect to the device manager.

If you remain connected to the device manager after the **Saving Management Center/CDO Registration Settings** step, you will eventually see the **Successful Connection with Management Center or CDO** dialog box, after which you will be disconnected from the device manager.

Figure 112: Successful Connection

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. You configured basic settings for the outside interface as part of the manager access setup, but you still need to assign it to a security zone.

- DHCP server—Use a DHCP server on the inside interface for clients.

- NAT—Use interface PAT on the outside interface.

- Access control—Allow traffic from inside to outside.

- SSH—Enable SSH on the manager access interface.

Configure Interfaces

When you use zero-touch provisioning or the device manager for initial setup, the following interfaces are preconfigured:

- Ethernet 1/1—"outside", IP address from DHCP, IPv6 autoconfiguration

- Ethernet 1/2— "inside", 192.168.95.1/24

- Default route—Obtained through DHCP on the outside interface

If you performed additional interface-specific configuration within device manager before registering with the management center, then that configuration is preserved.

In any case, you need to perform additional interface configuration after you register the device. Enable the threat defense interfaces, assign them to security zones, and set the IP addresses. Also configure breakout 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 **Edit** (✐) for the firewall.

Step 2   Click **Interfaces**.

Figure 113: Interfaces

Step 3   To create 4 x 10-Gb breakout interfaces from a 40-Gb interface (available on some models), click the breakout icon for the interface.

If you already used the 40-Gb interface in your configuration, you will have to remove the configuration before you can proceed with the breakout.

Step 4   Click **Edit** (✐) for the interface that you want to use for *inside*.

The **General** tab appears.

Figure 114: General Tab

Edit Physical Interface

| General | IPv4 | IPv6 | Path Monitoring | H |

Name:

inside

☑ Enabled

☐ Management Only

Description:

Mode:

None ▾

Security Zone:

inside_zone ▾

Interface ID:

GigabitEthernet0/1

MTU:

1500

(64 - 9000)

Priority:

0   *(0 - 65535)*

Propagate Security Group Tag: ☐

NVE Only:

☐

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**

Figure 115: IPv4 Tab

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

Figure 116: IPv6 Tab

  f) Click **OK**.

Step 5 Click **Edit** (✐) for the interface that you want to use for *outside*.

The **General** tab appears.

Figure 117: General Tab

You already pre-configured this interface for manager access, so the interface will already be named, enabled, and addressed. You should not alter any of these basic settings because doing so will disrupt the management center management connection. You must still configure the Security Zone on this screen for through traffic policies.

a) 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**.

b) Click **OK**.

Step 6   Click **Save**.

Configure the DHCP Server

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

Procedure

Step 1   Choose **Devices** > **Device Management**, and click **Edit** (✎) for the device.

Step 2   Choose **DHCP** > **DHCP Server**.

Figure 118: DHCP Server

Step 3   On the **Server** page, click **Add**, and configure the following options:

Figure 119: Add Server

- **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**.

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**.

Figure 120: New Policy

The policy is added the management center. You still have to add rules to the policy.

Figure 121: NAT Policy
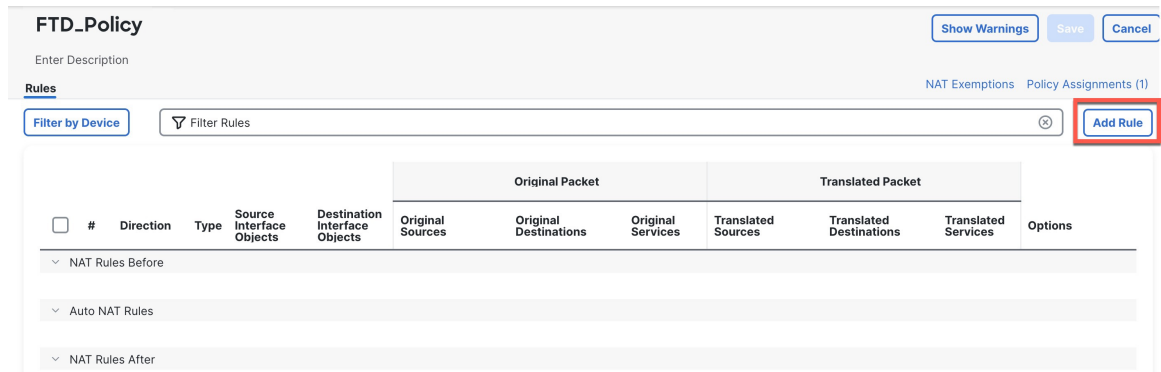
Step 3   Click **Add Rule**.

The **Add NAT Rule** dialog box appears.

Step 4   Configure the basic rule options:

Figure 122: Basic Rule Options
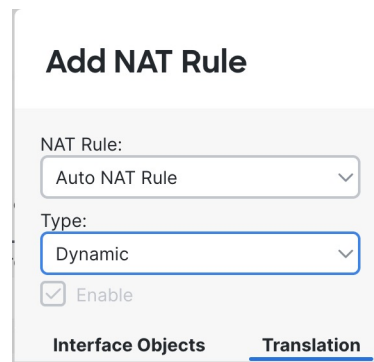
• **NAT Rule**—Choose **Auto NAT Rule**.

• **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.

Figure 123: Interface Objects
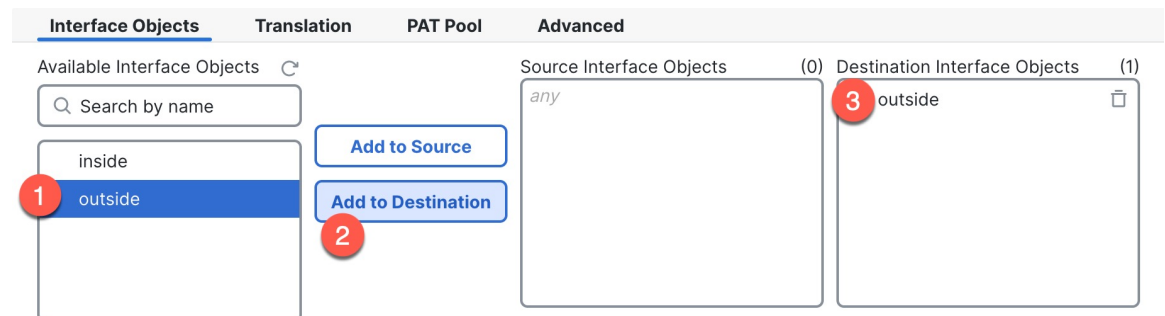
Step 6 On the **Translation** page, configure the following options:

Figure 124: Translation

Interface Objects	Translation	PAT Pool	Advanced

Original Packet

Translated Packet

Original Source:*

all-ipv4 ⌄   +

Translated Source:

Destination Interface IP ⌄

ⓘ The values selected for Destination Interface Objects in 'Interface Objects' tab will be used

Original Port:

TCP ⌄

Translated Port:

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

Figure 125: New Network Object

New Network Object ⓘ

Name

all-ipv4

Description

Network

○ Host   ○ Range   ● Network   ○ FQDN

0.0.0.0/0

☐ **Allow Overrides**

Cancel   **Save**

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 threat defense, 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.

Procedure

Step 1   Choose **Policy** > **Access Policy** > **Access Policy**, and click **Edit** (✐) for the access control policy assigned to the threat defense.

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

Figure 126: Source Zone
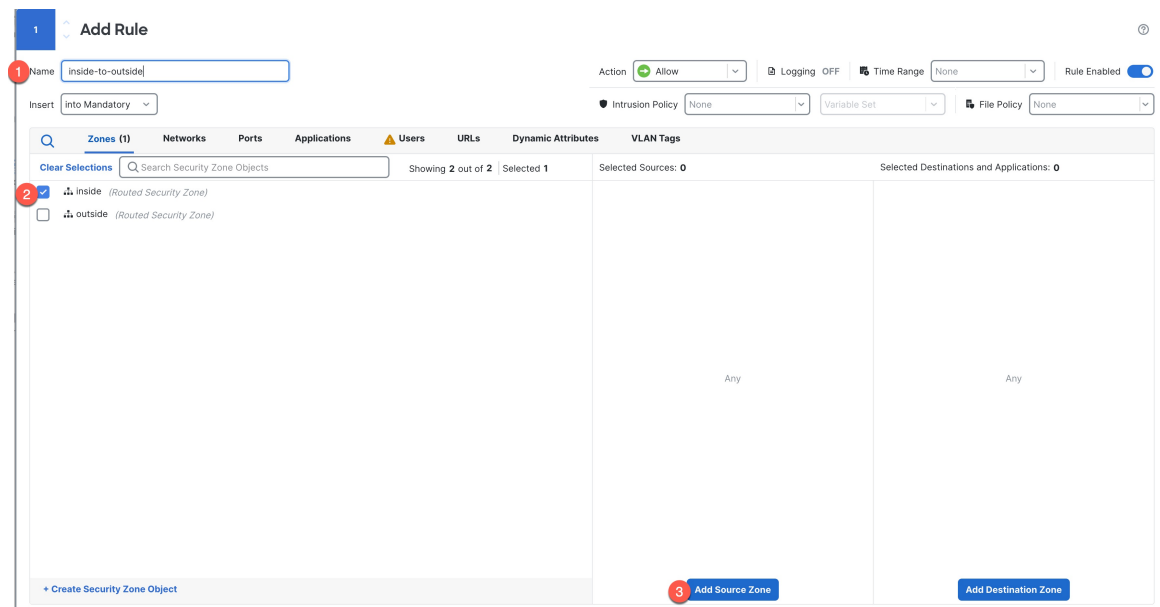
Figure 127: Destination Zone

Figure 128: Apply

- **Name**—Name this rule, for example, **inside-to-outside**.

- **Selected Sources**—Select the inside zone from **Zones**, and click **Add Source Zone**.

- **Selected Destinations and Applications**—Select the outside zone from **Zones**, and click **Add Destination Zone**.

Leave the other settings as is.

Step 3 Click **Apply**.

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

Step 4 Click **Save**.

Configure SSH on the Manager Access Data Interface

If you enabled management center access on a data interface, such as outside, you should enable SSH on that interface using this procedure. This section describes how to enable SSH connections to one or more *data* interfaces on the threat defense. SSH is not supported to the Diagnostic logical interface.

The threat defense uses the CiscoSSH stack, which is based on OpenSSH. CiscoSSH supports FIPS compliance and regular updates, including updates from Cisco and the open source community.

Note SSH is enabled by default on the Management interface; however, this screen does not affect Management SSH access.

The Management interface is separate from the other interfaces on the device. It is used to set up and register the device to the management center. SSH for data interfaces shares the internal and external user list with SSH for the Management interface. Other settings are configured separately: for data interfaces, enable SSH and access lists using this screen; SSH traffic for data interfaces uses the regular routing configuration, and not any static routes configured at setup or at the CLI.

For the Management interface, to configure an SSH access list, see the **configure ssh-access-list** command in the Cisco Secure Firewall Threat Defense Command Reference. To configure a static route, see the **configure network static-routes** command. By default, you configure the default route through the Management interface at initial setup.

To use SSH, you do not also need an access rule allowing the host IP address. You only need to configure SSH access according to this section.

You can SSH only to a reachable interface (including an interface in a user-defined virtual router); if your SSH host is located on the outside interface, you can only initiate a management connection directly to the outside interface. When you enable SSH in a user-defined virtual router, and you want VPN users to access SSH, be sure to terminate the VPN on the same virtual router. If the VPN is terminated on another virtual router, then you must configure route leaks between the virtual routers.

SSH supports the following ciphers and key exchange:

- Encryption—aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr

- Integrity—hmac-sha2-256

- Key exchange—dh-group14-sha256

Note After you make three consecutive failed attempts to log into the CLI using SSH, the device terminates the SSH connection.

Before you begin

- You can configure SSH internal users at the CLI using the **configure user add** command. By default, there is an **admin** user for which you configured the password during initial setup. You can also configure external users on LDAP or RADIUS by configuring **External Authentication** in platform settings.

- You need network objects that define the hosts or networks you will allow to make SSH connections to the device. You can add objects as part of the procedure, but if you want to use object groups to identify a group of IP addresses, ensure that the groups needed in the rules already exist. Select **Objects** > **Object Management** to configure objects.

> **Note** You cannot use the system-provided **any** network object. Instead, use **any-ipv4** or **any-ipv6**.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the threat defense policy.

Step 2 Select **Secure Shell**.

Step 3 Identify the interfaces and IP addresses that allow SSH connections.

Use this table to limit which interfaces will accept SSH connections, and the IP addresses of the clients who are allowed to make those connections. You can use network addresses rather than individual IP addresses.

a) Click **Add** to add a new rule, or click **Edit** to edit an existing rule.

b) Configure the rule properties:

- **IP Address**—The network object or group that identifies the hosts or networks you are allowing to make SSH connections. Choose an object from the drop-down menu, or click + to add a new network object.

- **Security Zones**—Add the zones that contain the interfaces to which you will allow SSH connections. For interfaces not in a zone, you can type the interface name into the field below the **Selected Security Zones** list and click **Add**. These rules will be applied to a device only if the device includes the selected interfaces or zones.

c) Click **OK**.

Step 4 Click **Save**.

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

Deploy the Configuration

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

Procedure

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

Figure 129: Deploy
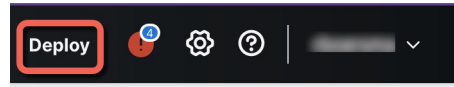
Step 2   For a quick deployment, check specific devices and then click **Deploy**, or click **Deploy All** to deploy to all
devices. Otherwise, for additional deployment options, click **Advanced Deploy**.

Figure 130: Deploy Selected
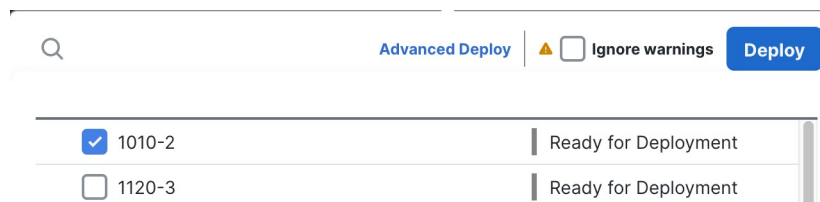
Figure 131: Deploy All
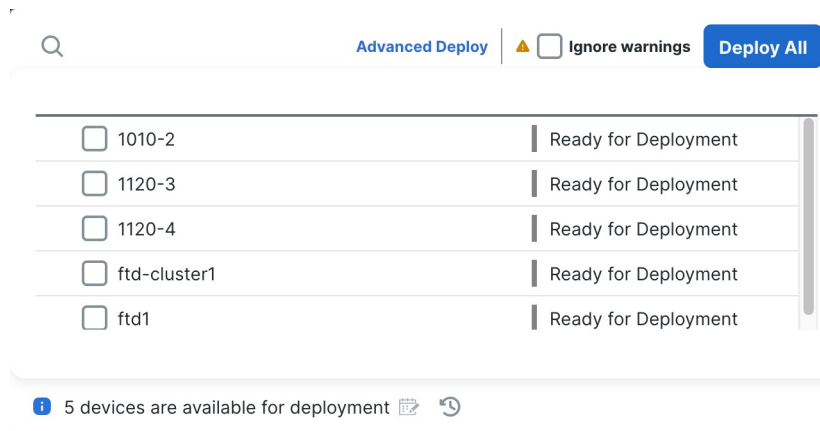
Figure 132: Advanced Deploy
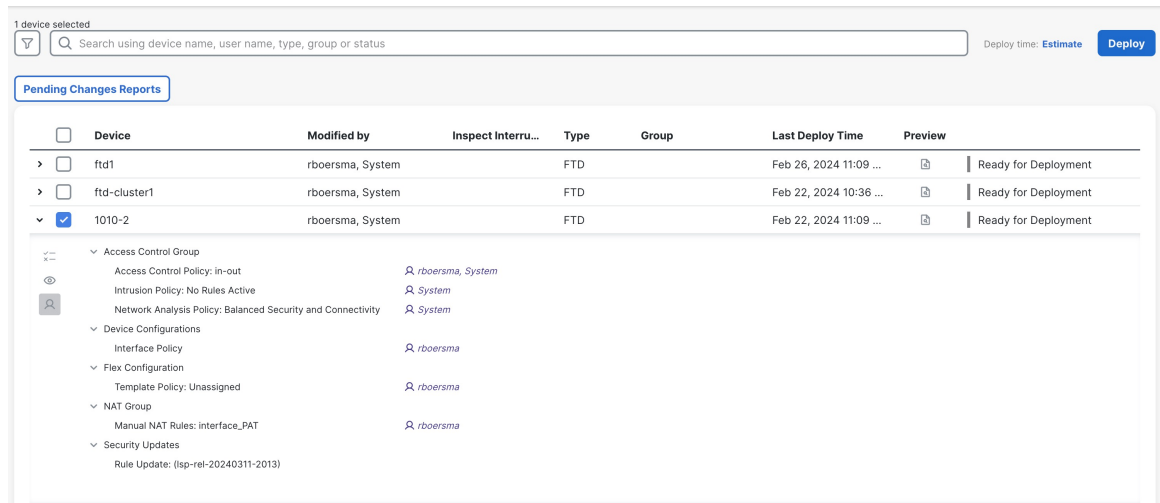
Step 3 Ensure that the deployment succeeds. Click the icon to the right of the **Deploy** button in the menu bar to see status for deployments.

Figure 133: Deployment Status

Access the Threat Defense and FXOS 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 also access the FXOS CLI for troubleshooting purposes.

Note You can alternatively SSH to the Management interface of the threat defense device. Unlike a console session, the SSH session defaults to the threat defense CLI, from which you can connect to the FXOS CLI using the **connect fxos** command. You can later 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. This procedure describes console port access, which defaults to the FXOS CLI.

Procedure

Step 1 To log into the CLI, connect your management computer to the console port. The Secure Firewall 3100 ships with a DB-9 to RJ-45 serial cable, so you may need to buy a third party DB-9-to-USB serial cable to make the connection. Be sure to install any necessary USB serial drivers for your operating system. The console port defaults to the FXOS CLI. Use the following serial settings:

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

You connect to the FXOS CLI. Log in to the CLI using the **admin** username and the password you set at initial setup (the default is **Admin123**).

Example:

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

Step 2 Access the threat defense CLI.

connect ftd

Example:

```
firepower# connect ftd
>
```

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

Step 3 To exit the threat defense CLI, enter the **exit** or **logout** command.

This command returns you to the FXOS CLI prompt. For information on the commands available in the FXOS CLI, enter **?**.

Example:

```
> exit
firepower#
```

Power Off the Firewall

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 firewall system.

You can power off the device using the management center device management page, or you can use the FXOS CLI.

Power Off the Firewall Using CDO

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 firewall.

You can shut down your system properly using the management center.

Procedure

Step 1   Choose **Devices** > **Device Management**.

Step 2   Next to the device that you want to restart, click **Edit** (✎).

Step 3   Click the **Device** tab.

Step 4   Click **Shut Down Device** (✖) in the **System** section.

Step 5   When prompted, confirm that you want to shut down the device.

Step 6   If you have a console connection to the firewall, monitor the system prompts as the firewall shuts down. You will see the following prompt:

```
System is stopped.
It is safe to power off now.

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

If you do not have a console connection, wait approximately 3 minutes to ensure the system has shut down.

Step 7   You can now turn off the power switch and unplug the power to physically remove power from the chassis if necessary.

Power Off the Firewall at the CLI

You can use the FXOS CLI to safely shut down the system and power off the device. You access the CLI by connecting to the console port; see Access the Threat Defense and FXOS CLI, on page 166.

Procedure

Step 1   In the FXOS CLI, connect to local-mgmt:

firepower # **connect local-mgmt**

Step 2   Issue the **shutdown** command:

firepower(local-mgmt) # **shutdown**

Example:

```
firepower(local-mgmt)# shutdown
This command will shutdown the system.  Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense......ok
```

Step 3   Monitor the system prompts as the firewall shuts down. You will see the following prompt:

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

Step 4   You can now turn off the power switch and unplug the power to physically remove power from the chassis if necessary.

What's Next

To continue configuring your threat defense using CDO, see the Cisco Defense Orchestrator home page.

ASA Deployment with ASDM

Is This Chapter for You?

To see all available operating systems and managers, see Which Application and Manager is Right for You?, on page 1. This chapter applies to ASA using ASDM.

About the Firewall

The hardware can run either threat defense software or ASA software. Switching between threat defense and ASA requires you to reimage the device. You should also reimage if you need a different software version than is currently installed. See Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.

The firewall runs an underlying operating system called the Secure Firewall eXtensible Operating System (FXOS). The firewall does not support the FXOS Secure Firewall chassis manager; only a limited CLI is supported for troubleshooting purposes. See the Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 and Secure Firewall 3100/4200 with Firepower Threat Defense for more information.

Privacy Collection Statement—The firewall 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 the ASA

The ASA provides advanced stateful firewall and VPN concentrator functionality in one device.

Migrating an ASA 5500-X Configuration

You can copy and paste an ASA 5500-X configuration into the Secure Firewall 3100. However, you will need to modify your configuration. Also note some behavioral differences between the platforms.

1. To copy the configuration, enter the **more system:running-config** command on the ASA 5500-X.

2. Edit the configuration as necessary (see below).

3. Connect to the console port of the Secure Firewall 3100, and enter global configuration mode:

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa# configure terminal
ciscoasa(config)#
```

4. Clear the current configuration using the **clear configure all** command.

5. Paste the modified configuration at the ASA CLI.

This guide assumes a factory default configuration, so if you paste in an existing configuration, some of the procedures in this guide will not apply to your ASA.

ASA 5500-X Configuration	Secure Firewall 3100 Configuration
PAK License	Smart License PAK licensing is not applied when you copy and paste your configuration. There are no licenses installed by default. Smart Licensing requires that you connect to the Smart Licensing server to obtain your licenses. Smart Licensing also affects ASDM or SSH access (see below).
Initial ASDM access	Remove any VPN or other strong encryption feature configuration—even if you only configured weak encryption—if you cannot connect to ASDM or register with the Smart Licensing server. You can reenable these features after you obtain the Strong Encryption (3DES) license. The reason for this issue is that the ASA includes 3DES capability by default for management access only. If you enable a strong encryption feature, then ASDM and HTTPS traffic (like that to and from the Smart Licensing server) are blocked. The exception to this rule is if you are connected to a management-only interface, such as Management 1/1. SSH is not affected.
Interface IDs	Make sure you change the interface IDs to match the new hardware IDs. For example, the ASA 5525-X includes Management 0/0, and GigabitEthernet 0/0 through 0/5. The Firepower 1120 includes Management 1/1 and Ethernet 1/1 through 1/8.

ASA 5500-X Configuration	Secure Firewall 3100 Configuration
boot system commands The ASA 5500-X allows up to four **boot system** commands to specify the booting image to use.	The Secure Firewall 3100 only allows a single **boot system** command, so you should remove all but one command before you paste. You actually do not need to have *any* **boot system** commands present in your configuration, as it is not read at startup to determine the booting image. The last-loaded boot image will always run upon reload. The **boot system** command performs an action when you enter it: the system validates and unpacks the image and copies it to the boot location (an internal location on disk0 managed by FXOS). The new image will load when you reload the ASA.

End-to-End Tasks

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

Figure 134: End-to-End Procedure
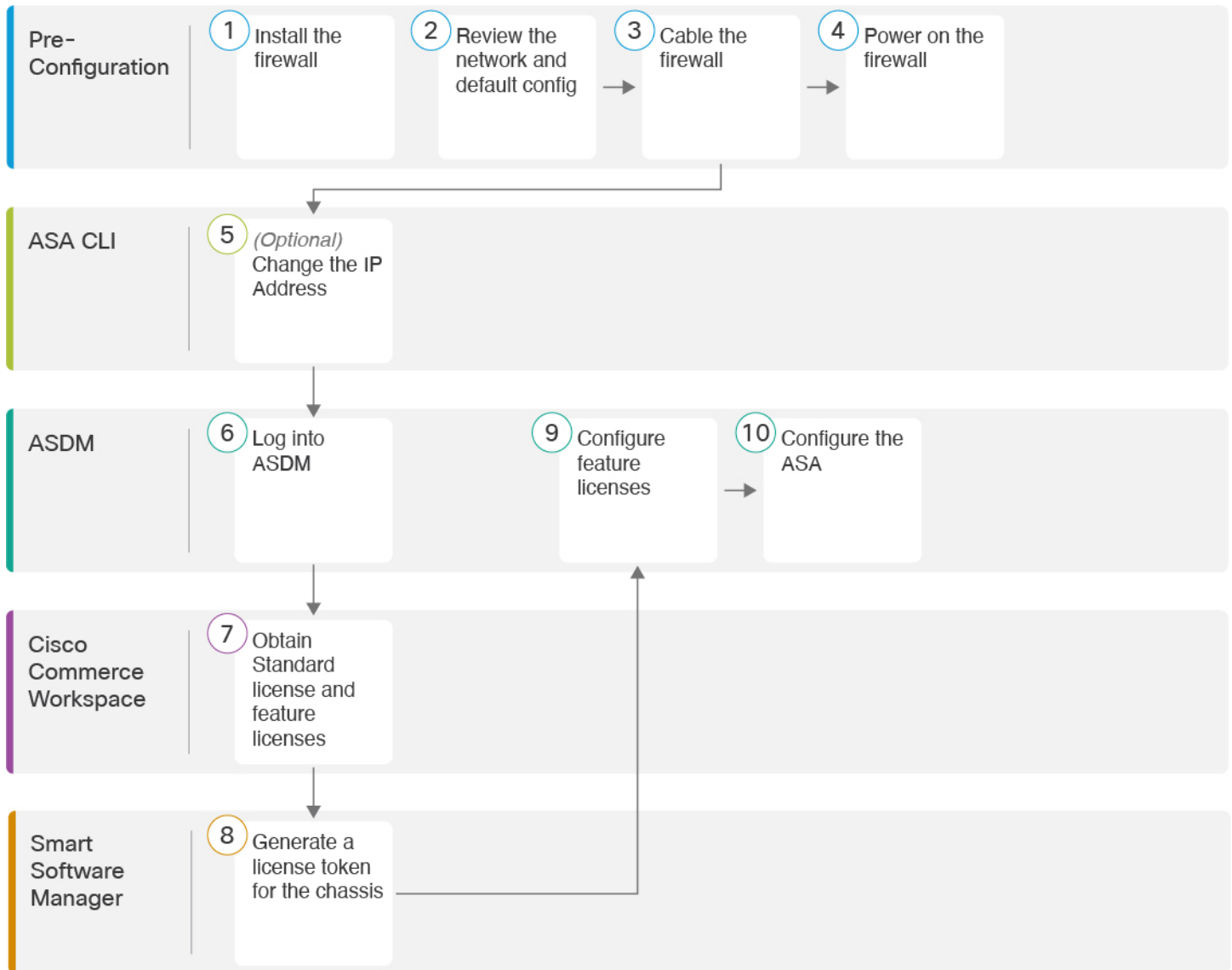
1	Pre-Configuration	Install the firewall. See the hardware installation guide.
2	Pre-Configuration	Review the Network Deployment and Default Configuration, on page 175.
3	Pre-Configuration	Cable the Firewall, on page 177.
4	Pre-Configuration	Power on the Firewall, on page 178.
5	ASA CLI	(Optional) Change the IP Address, on page 179.

6	ASDM	Log Into ASDM, on page 180.
7	Cisco Commerce Workspace	Obtain Standard license and optional feature licenses (Configure Licensing, on page 181).
8	Smart Software Manager	Generate a license token for the chassis (Configure Licensing, on page 181).
9	ASDM	Configure feature licenses (Configure Licensing, on page 181).
10	ASDM	Configure the ASA, on page 187.

Review the Network Deployment and Default Configuration

The following figure shows the default network deployment for the ASA using the default configuration.

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 ASA 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 as part of the ASDM Startup Wizard.

Note   If you cannot use the default Management IP address for ASDM access, you can set the Management IP address at the ASA CLI. See (Optional) Change the IP Address, on page 179.

If you need to change the inside IP address, you can do so using the ASDM Startup Wizard. For example, you may need to change the inside IP address in the following circumstances:

- 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 ASA 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 ASA to an existing inside network, you will need to change the inside IP address to be on the existing network.

Management Computer
DHCP from inside ifc: 192.168.1.x
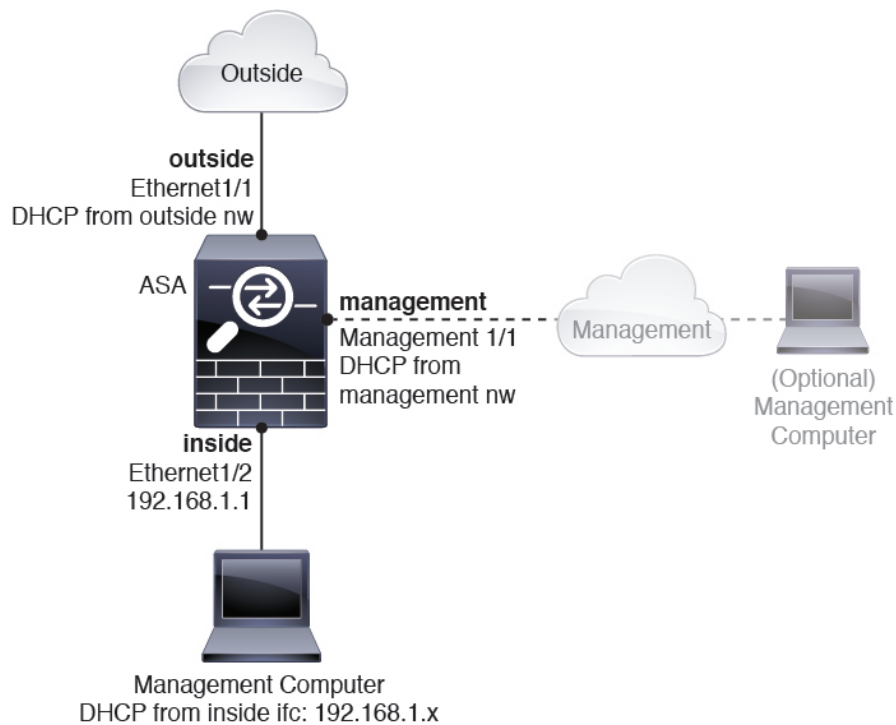
Secure Firewall 3100 Default Configuration

The default factory configuration for the Secure Firewall 3100 configures the following:

- **inside→outside traffic flow**—Ethernet 1/1 (outside), Ethernet 1/2 (inside)

- **outside IP address** from DHCP, **inside IP address**—192.168.1.1

- **management**—Management 1/1 (management), IP address from DHCP

- **DHCP server** on inside interface

- **Default routes** from outside DHCP, management DHCP

- **ASDM** access—Management and inside hosts allowed. Inside hosts are limited to the 192.168.1.0/24 network.

- **NAT**—Interface PAT for all traffic from inside to outside.

- **DNS** servers—OpenDNS servers are pre-configured.

The configuration consists of the following commands:

```
interface Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/1
```

```
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Cable the Firewall

Figure 135: Cabling the Secure Firewall 3100
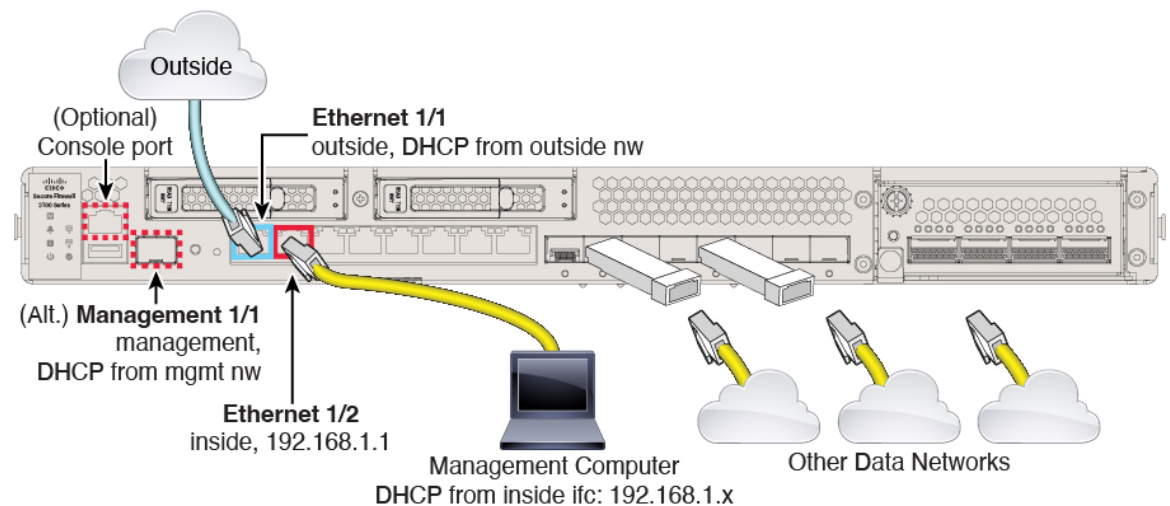
Manage the Secure Firewall 3100 on either Management 1/1 or Ethernet 1/2. The default configuration also configures Ethernet1/1 as outside.

Before you begin

- Install an SFP for the Management port—The Management port is a 1/10-Gb SFP port that requires an SFP module.

- Obtain a console adapter—The Secure Firewall 3100 ships with a DB-9 to RJ-45 serial cable, so you may need to buy a third party DB-9-to-USB serial cable to make the connection.

Procedure

Step 1 Install the chassis. See the hardware installation guide.

Step 2 Connect your management computer to either of the following interfaces:

- **Ethernet 1/2**—Ethernet 1/2 has a default IP address (192.168.1.1) 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 (see Secure Firewall 3100 Default Configuration, on page 176). Only clients on 192.168.1.0/24 can access the ASA.

    If you need to change the Ethernet 1/2 IP address from the default, you must also cable your management computer to the console port. See (Optional) Change the IP Address, on page 179.

- **Management 1/1**—Management 1/1 obtains an IP address from a DHCP server on your management network; if you use this interface, you must determine the IP address assigned to the ASA so that you can connect to the IP address from your management computer.

You can later configure ASA management access from other interfaces; see the ASA general operations configuration guide.

Step 3 Connect the outside network to the Ethernet1/1 interface.

For Smart Software Licensing, the ASA needs internet access.

**Step 4** Connect other networks to the remaining interfaces.

Power on the Firewall

System power is controlled by a rocker power switch located on the rear of the firewall. The power switch is implemented as a soft notification switch that supports graceful shutdown of the system to reduce the risk of system software and data corruption.

Procedure

Step 1 Attach the power cord to the firewall, 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 back of the firewall; if it is solid green, the firewall is powered on.

Figure 136: System and Power LEDs
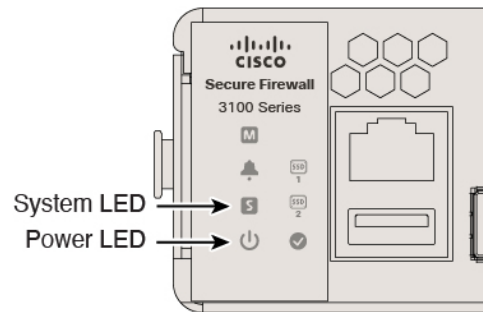
Step 4 Check the System LED on the back of the firewall; after it is solid green, the system has passed power-on diagnostics.

> **Note** When the switch is toggled from ON to OFF, it may take several seconds for the system to eventually power off. During this time, the Power LED on the front of the chassis blinks green. Do not remove the power until the Power LED is completely off.

(Optional) Change the IP Address

If you cannot use the default IP address for ASDM access, you can set the IP address of the inside interface at the ASA CLI.

> **Note** This procedure restores the default configuration and also sets your chosen IP address, so if you made any changes to the ASA configuration that you want to preserve, do not use this procedure.

Procedure

Step 1 Connect to the ASA console port, and enter global configuration mode. See Access the ASA and FXOS CLI, on page 188 for more information.

Step 2 Restore the default configuration with your chosen IP address.

configure factory-default [*ip_address* [*mask*]]

Example:

```
ciscoasa(config)# configure factory-default 10.1.1.151 255.255.255.0
Based on the management IP address and mask, the DHCP address
pool size is reduced to 103 from the platform limit 256

WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.
```

```
Begin to apply factory-default configuration:
Clear all configuration
Executing command: interface ethernet1/2
Executing command: nameif inside
INFO: Security level for "inside" set to 100 by default.
Executing command: ip address 10.1.1.151 255.255.255.0
Executing command: security-level 100
Executing command: no shutdown
Executing command: exit
Executing command: http server enable
Executing command: http 10.1.1.0 255.255.255.0 management
Executing command: dhcpd address 10.1.1.152-10.1.1.254 management
Executing command: dhcpd enable management
Executing command: logging asdm informational
Factory-default configuration is completed
ciscoasa(config)#
```

Step 3 Save the default configuration to flash memory.

write memory

Log Into ASDM

Launch ASDM so you can configure the ASA.

The ASA includes 3DES capability by default for management access only, so you can connect to the Smart Software Manager and also use ASDM immediately. You can also use SSH and SCP if you later configure SSH access on the ASA. Other features that require strong encryption (such as VPN) must have Strong Encryption enabled, which requires you to first register to the Smart Software Manager.

Note If you attempt to configure any features that can use strong encryption before you register—even if you only configure weak encryption—then your HTTPS connection will be dropped on that interface, and you cannot reconnect. The exception to this rule is if you are connected to a management-only interface, such as Management 1/1. SSH is not affected. If you lose your HTTPS connection, you can connect to the console port to reconfigure the ASA, connect to a management-only interface, or connect to an interface not configured for a strong encryption feature.

Before you begin

• See the ASDM release notes on Cisco.com for the requirements to run ASDM.

Procedure

Step 1 Enter the following URL in your browser.

• **https://192.168.1.1**—Inside (Ethernet 1/2) interface IP address.

• **https://***management_ip*—Management interface IP address assigned from DHCP.

| Note | Be sure to specify **https://**, and not **http://** or just the IP address (which defaults to HTTP); the ASA does not automatically forward an HTTP request to HTTPS. |

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 **Install ASDM Launcher**.

Step 3   Follow the onscreen instructions to launch ASDM.

The **Cisco ASDM-IDM Launcher** appears.

Step 4   Leave the username and password fields empty, and click **OK**.

The main ASDM window appears.

Configure Licensing

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

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

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

- Essentials

- Security Contexts

- Carrier—Diameter, GTP/GPRS, M3UA, SCTP

- Strong Encryption (3DES/AES)—If your Smart Account is not authorized for strong encryption, but Cisco has determined that you are allowed to use strong encryption, you can manually add a stong encryption license to your account.

- Cisco Secure Client—Secure Client Advantage, Secure Client Premier, or Secure Client VPN Only.

The ASA includes 3DES capability by default for management access only, so you can connect to the Smart Software Manager and also use ASDM immediately. You can also use SSH and SCP if you later configure SSH access on the ASA. Other features that require strong encryption (such as VPN) must have Strong Encryption enabled, which requires you to first register to the Smart Software Manager.

Note   If you attempt to configure any features that can use strong encryption before you register—even if you only configure weak encryption—then your HTTPS connection will be dropped on that interface, and you cannot reconnect. The exception to this rule is if you are connected to a management-only interface, such as Management 1/1. SSH is not affected. If you lose your HTTPS connection, you can connect to the console port to reconfigure the ASA, connect to a management-only interface, or connect to an interface not configured for a strong encryption feature.

When you request the registration token for the ASA from the Smart Software Manager, 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. If your Smart Account is not authorized for strong encryption, but Cisco has determined that you are allowed to use strong encryption, you can manually add a strong encryption license to your account.

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 Manager 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, including at a minimum the Essentials 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 **Search All** field on the Cisco Commerce Workspace.
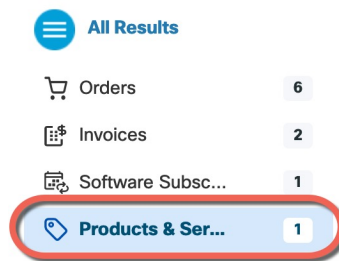
Figure 137: License Search
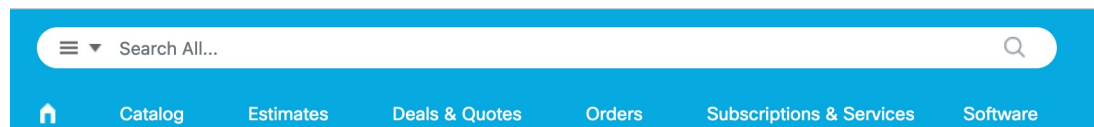
Choose **Products & Services** from the results.

Figure 138: Results

All Results

🛒 Orders   6

📑$ Invoices   2

🗃️ Software Subsc...   1

🏷️ **Products & Ser...**   **1**
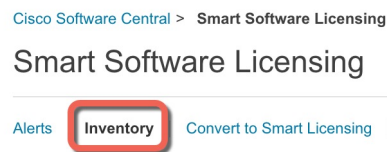
Search for the following license PIDs:

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

- Essentials—*Included automatically*.

- 5 context—L-FPR3K-ASASC-5=. Context licenses are additive; buy multiple licenses.

- 10 context—L-FPR3K-ASASC-10=. Context licenses are additive; buy multiple licenses.

- Carrier (Diameter, GTP/GPRS, M3UA, SCTP)—L-FPR3K-ASA-CAR=

- Strong Encryption (3DES/AES)—L-FPR3K-ENC-K9=. Only required if your account is not authorized for strong encryption.

- Cisco Secure Client—See the Cisco Secure Client 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**.

Cisco Software Central > **Smart Software Licensing**

Smart Software Licensing

Alerts   **Inventory**   Convert to Smart Licensing |
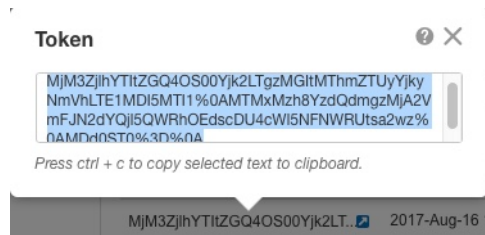
b) On the **General** tab, click **New Token**.

Product Instance Registration Tokens

The registration tokens below can be used to register new product instances t

New Token...

Token | Expiration Date | Uses

OWFlNTZiYTgtY2Ew… 🔗 2024-May-18 17:41:53 (in 30 days)   0 of 10

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

- **Description**

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

- **Max. Number of Uses**

- **Allow export-controlled functionaility 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.

Figure 139: View Token

Figure 140: Copy Token

Step 3   In ASDM, choose **Configuration** > **Device Management** > **Licensing** > **Smart Licensing**.

Step 4   Click **Register**.

**Step 5**   Enter the registration token in the **ID Token** field.
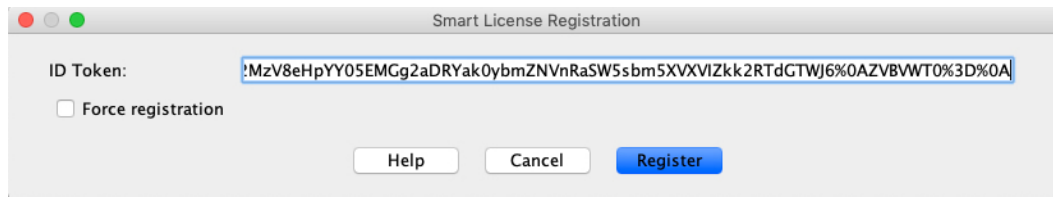
You can optionally check the **Force registration** check box to register the ASA that is already registered, but that might be out of sync with the Smart Software Manager. For example, use **Force registration** if the ASA was accidentally removed from the Smart Software Manager.

Step 6   Click **Register**.

The ASA registers with the Smart Software Manager using the pre-configured outside interface, and requests authorization for the configured license entitlements. The Smart Software Manager also applies the Strong Encryption (3DES/AES) license if your account allows. ASDM refreshes the page when the license status is updated. You can also choose **Monitoring** > **Properties** > **Smart License** to check the license status, particularly if the registration fails.
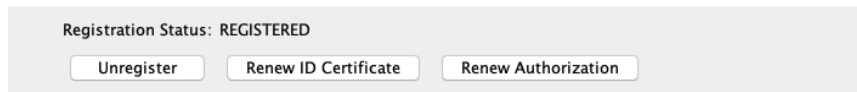
Step 7   Set the following parameters:
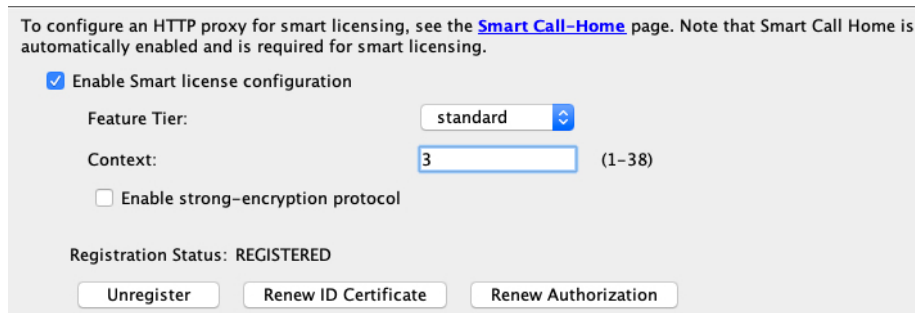
a)   Check **Enable Smart license configuration**.

b)   From the **Feature Tier** drop-down list, choose **Essentials**.

Only the Essentials tier is available.

c)   (Optional) For the **Context** license, enter the number of contexts.

You can use 2 contexts without a license. The maximum number of contexts depends on your model:

  • Secure Firewall 3100—100 contexts

For example, to use the maximum of 100 contexts on the Secure Firewall 3110, enter 98 for the number of contexts; this value is added to the default of 2.

Step 8   Click **Apply**.

Step 9   Click the **Save** icon in the toolbar.

**Step 10**   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.
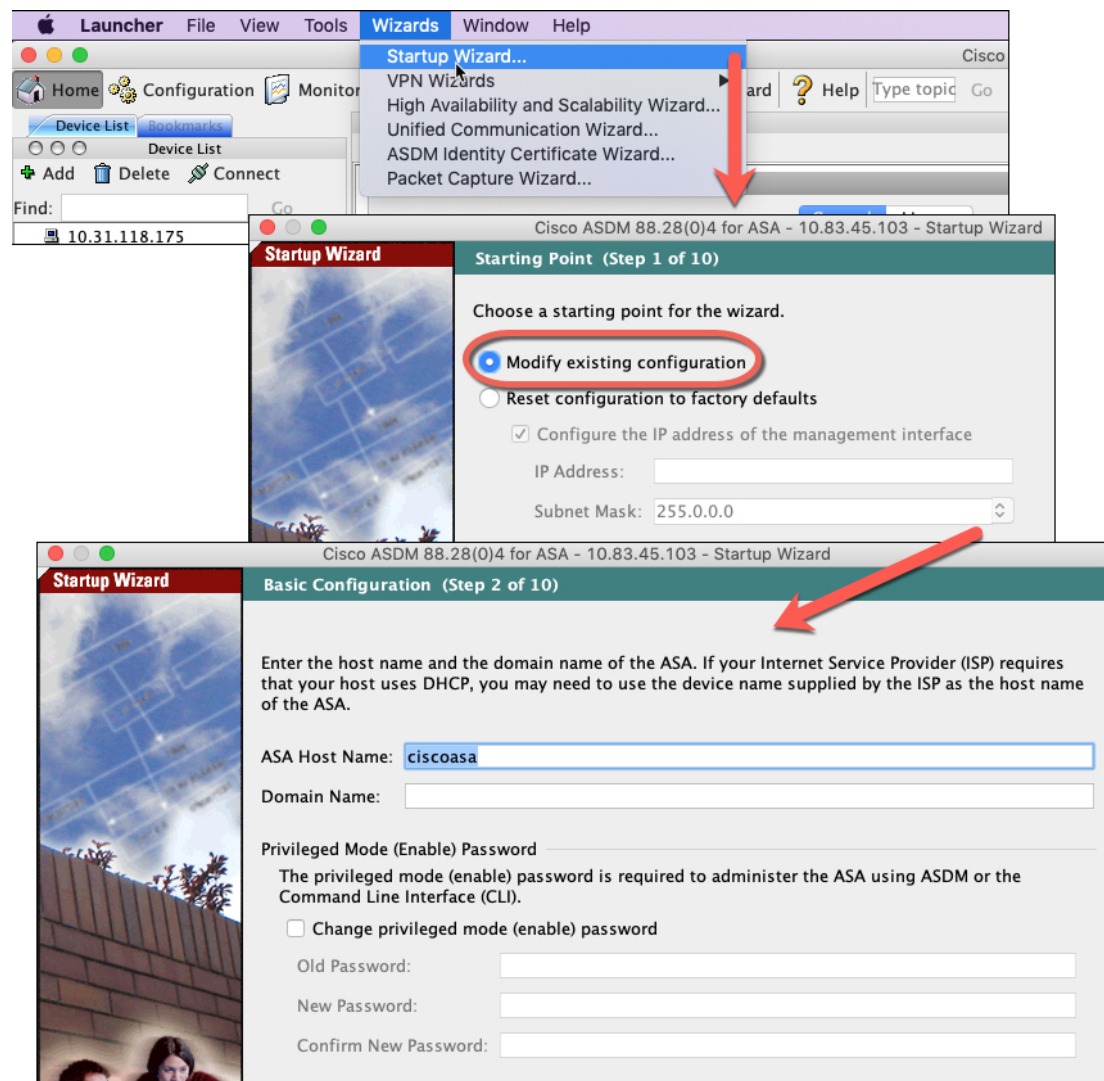
Step 2   The **Startup Wizard** walks you through configuring:

- 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 and FXOS CLI

You can use the ASA CLI to troubleshoot or configure the ASA instead of using ASDM. You can access the CLI by connecting to the console port. You can later configure SSH access to the ASA on any interface; SSH access is disabled by default. See the ASA general operations configuration guide for more information.

You can also access the FXOS CLI from the ASA CLI for troubleshooting purposes.

Procedure

Step 1   Connect your management computer to the console port. Be sure to install any necessary serial drivers for your operating system. Use the following serial settings:

- 9600 baud

- 8 data bits

- No parity

- 1 stop bit

You connect to the ASA CLI. There are no user credentials required for console access by default.

Step 2   Access privileged EXEC mode.

enable

You are prompted to change the password the first time you enter the **enable** command.

Example:

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa#
```

The enable password that you set on the ASA is also the FXOS **admin** user password if the ASA fails to boot up, and you enter FXOS failsafe mode.

All non-configuration commands are available in privileged EXEC mode. You can also enter configuration mode from privileged EXEC mode.

To exit privileged EXEC mode, enter the **disable**, **exit**, or **quit** command.

Step 3   Access global configuration mode.

configure terminal

Example:

```
ciscoasa# configure terminal
ciscoasa(config)#
```

You can begin to configure the ASA from global configuration mode. To exit global configuration mode, enter the **exit**, **quit**, or **end** command.

Step 4   (Optional) Connect to the FXOS CLI.

connect fxos [**admin**]

- **admin**—Provides admin-level access. Without this option, users have read-only access. Note that no configuration commands are available even in admin mode.

You are not prompted for user credentials. The current ASA username is passed through to FXOS, and no additional login is required. To return to the ASA CLI, enter **exit** or type **Ctrl-Shift-6**, **x**.

Within FXOS, you can view user activity using the **scope security/show audit-logs** command.

Example:

```
ciscoasa# connect fxos admin
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.
firepower#
firepower# exit
Connection with FXOS terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

What's Next?

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

- For troubleshooting, see the FXOS troubleshooting guide.