



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?](#). 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, on page 2](#)
- [End-to-End Tasks: Zero-Touch Provisioning, on page 3](#)
- [End-to-End Tasks: Onboarding Wizard, on page 5](#)
- [Central Administrator Pre-Configuration, on page 6](#)
- [Deploy the Firewall With Low-Touch Provisioning, on page 9](#)
- [Deploy the Firewall With the Onboarding Wizard, on page 15](#)
- [Configure a Basic Security Policy, on page 28](#)
- [Troubleshooting and Maintenance, on page 41](#)
- [What's Next, on page 49](#)

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 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.

High Availability Requirements

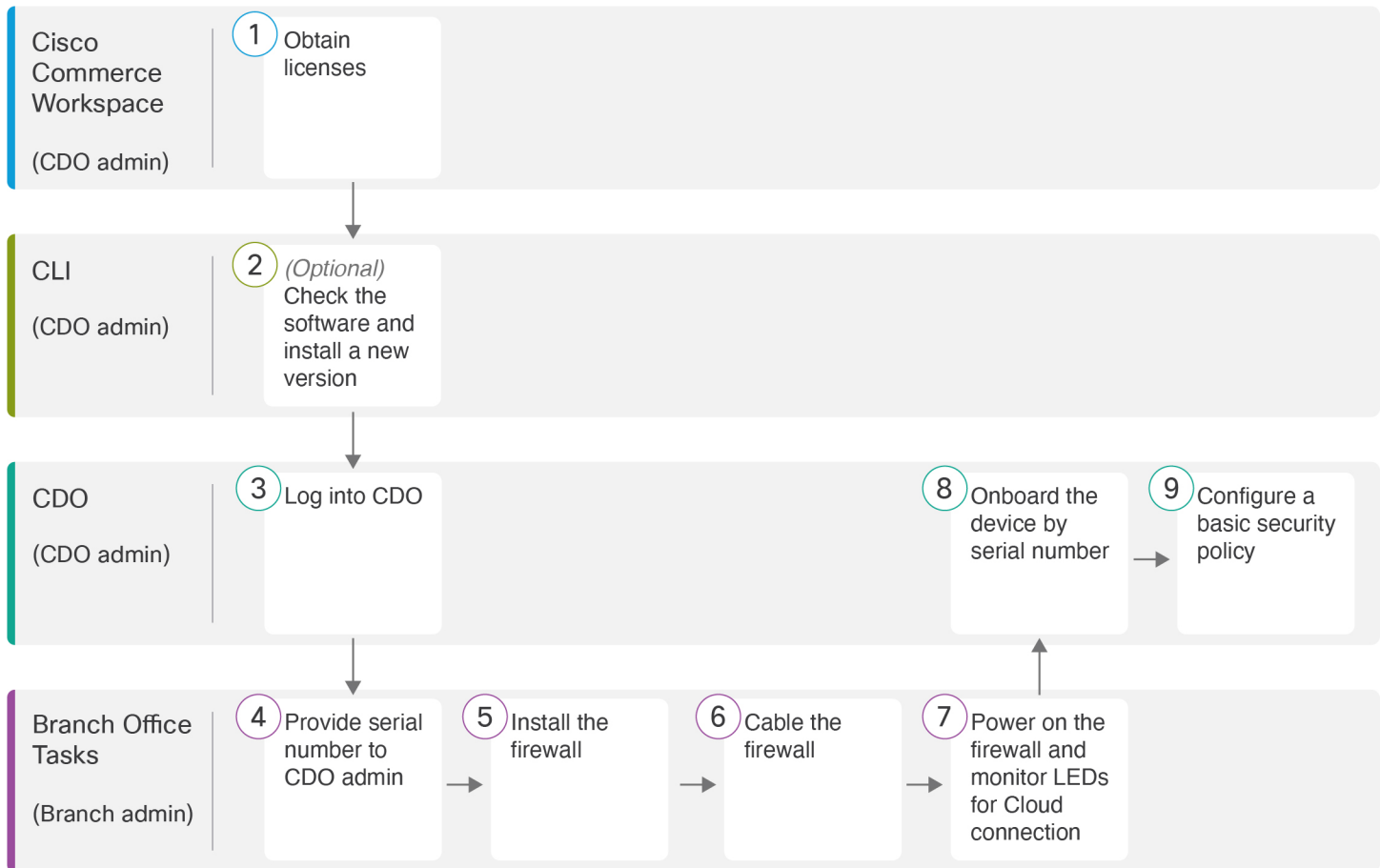
When using a data interface with device high availability, see the following requirements.

- Use the same data interface on both devices for manager access.
- Redundant manager access data interface is not supported.
- You cannot use DHCP; only a static IP address is supported. Features that rely on DHCP cannot be used, including DDNS and zero-touch provisioning.
- Have different static IP addresses in the same subnet.
- Use either IPv4 or IPv6; you cannot set both.
- Use the same manager configuration (**configure manager add** command) to ensure that the connectivity is the same.
- You cannot use the data interface as the failover or state link.

End-to-End Tasks: Zero-Touch Provisioning

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

Figure 1: End-to-End Tasks: Zero-Touch Provisioning



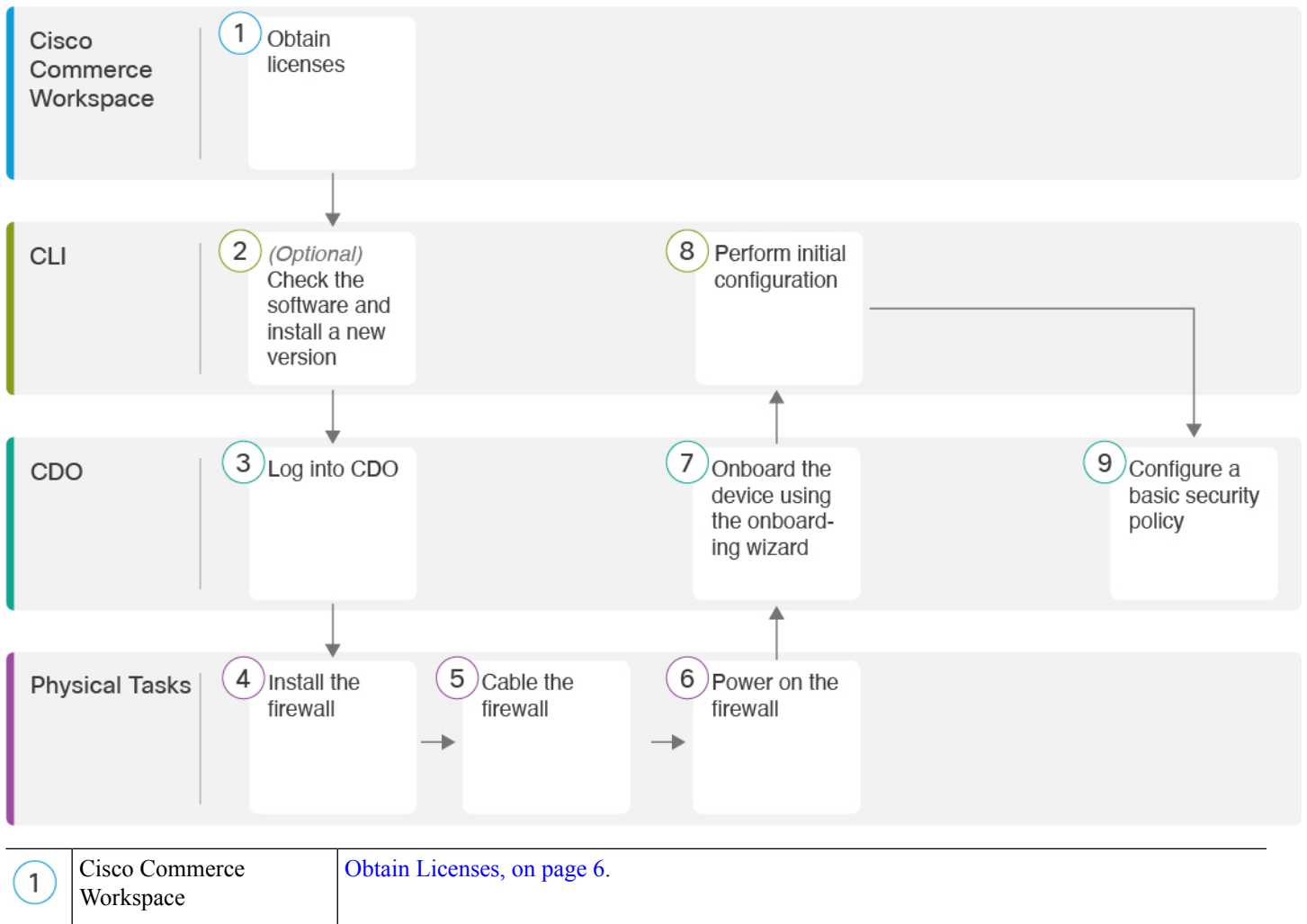
1	Cisco Commerce Workspace (CDO admin)	Obtain Licenses, on page 6.
2	CLI (CDO admin)	(Optional) Check the Software and Install a New Version, on page 8.
3	CDO (CDO admin)	Log Into CDO, on page 9.
4	Branch Office Tasks (Branch admin)	Provide the Firewall Serial Number to the Central Administrator, on page 10.
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 10.

7	Branch Office Tasks (Branch admin)	Power On the Firewall, on page 11.
8	CDO (CDO admin)	Onboard a Device with Zero-Touch Provisioning, on page 12.
9	CDO (CDO admin)	Configure a Basic Security Policy, on page 28.

End-to-End Tasks: Onboarding Wizard

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

Figure 2: End-to-End Tasks: Onboarding Wizard



2	CLI	(Optional) Check the Software and Install a New Version, on page 8.
3	CDO	Log Into CDO, on page 9.
4	Physical Tasks	Install the firewall. See the hardware installation guide .
5	Physical Tasks	Cable the Firewall , on page 15.
6	CDO	Onboard a Device with the Onboarding Wizard , on page 17.
7	CLI or Device Manager	<ul style="list-style-type: none"> • Perform Initial Configuration Using the CLI, on page 19. • Perform Initial Configuration Using the Device Manager, on page 24.
8	CDO	Configure a Basic Security Policy , on page 28.

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

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.

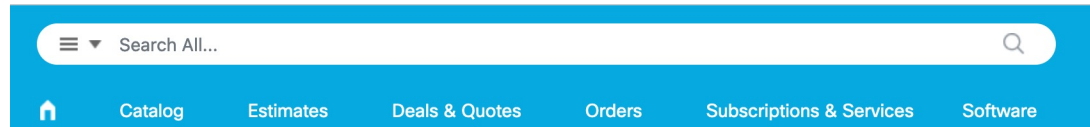
- Your Smart Software Licensing account must qualify for the Strong Encryption (3DES/AES) license to use some features (enabled using the export-compliance flag).

Procedure

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

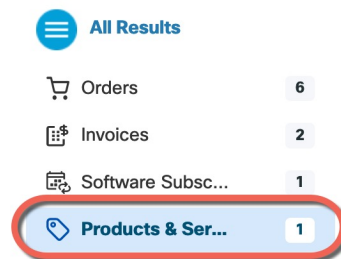
When you bought your device from Cisco or a reseller, your licenses should have been linked to your Smart Software License account. However, if you need to add licenses yourself, use the **Search All** field on the [Cisco Commerce Workspace](#).

Figure 3: License Search



Choose **Products & Services** from the results.

Figure 4: Results



Search for the following license PIDs:

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

- IPS, Malware Defense, and URL license combination:
 - L-FPR1120T-TMC=
 - L-FPR1140T-TMC=
 - L-FPR1150T-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-FPR1120T-TMC-1Y
- L-FPR1120T-TMC-3Y
- L-FPR1120T-TMC-5Y
- L-FPR1140T-TMC-1Y
- L-FPR1140T-TMC-3Y
- L-FPR1140T-TMC-5Y
- L-FPR1150T-TMC-1Y

- L-FPR1150T-TMC-3Y
- L-FPR1150T-TMC-5Y
- 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 16](#) and [Access the Threat Defense and FXOS CLI, on page 41](#) 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
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 19](#). 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 [Power Off the Device at the CLI, on page 48](#).

Log Into CDO

For details on creating a CDO tenant and logging in, see the CDO documentation: <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 administrator.

Procedure

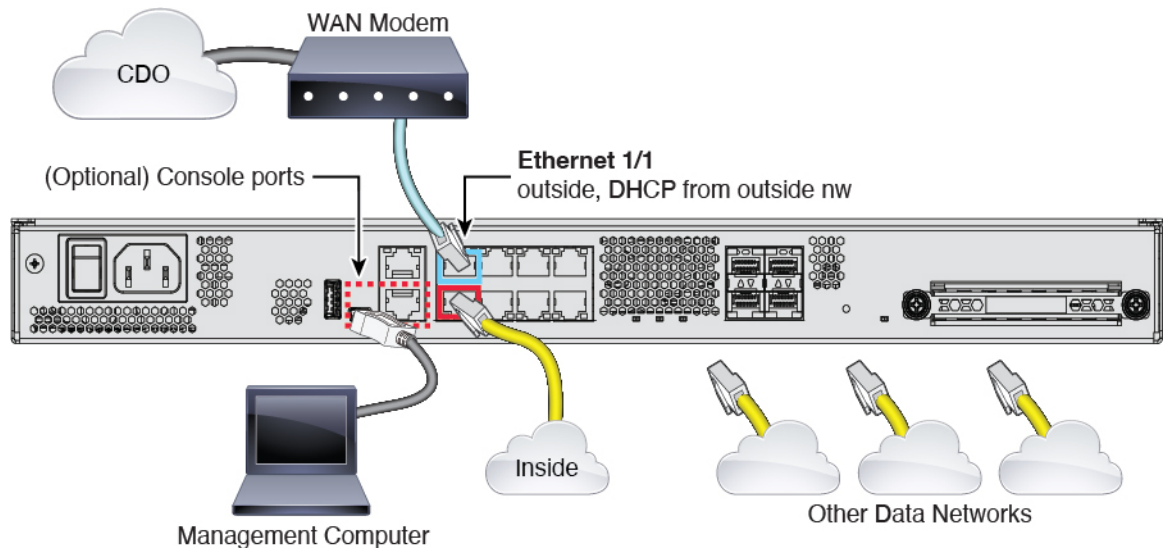
-
- Step 1** Unpack the chassis and chassis components.
- Take inventory of your firewall and packaging before you connect any cables or power on the firewall. You should also familiarize yourself with the chassis layout, components, and LEDs.
- Step 2** Record the firewall's serial number.
- The serial number of the firewall can be found on the shipping box. It can also be found on a sticker on the back of the firewall or on the bottom of the firewall chassis.
- 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

This topic describes how to connect the Firepower 1100 to your network 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 5: Cabling the Firepower 1100



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 device. 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.



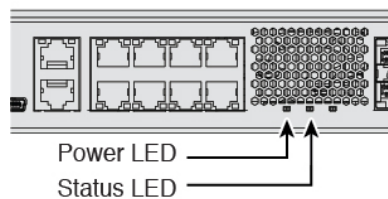
Note The first time you boot up the threat defense, initialization can take approximately 15 to 30 minutes.

Before you begin

It's important that you provide reliable power for your device (for example, using an uninterruptible 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 firewall system.

Procedure

-
- Step 1** Attach the power cord to the device, and connect it to an electrical outlet.
- Step 2** Turn the power on using the standard rocker-type power on/off switch located on the rear of the chassis, adjacent to the power cord.
- Step 3** Check the Power LED on the back of the device; if it is solid green, the device is powered on.



- Step 4** Check the Status LED on the back of the device; 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** Observe the Status LED on the back the device; when the device is booting correctly, the Status LED flashes fast green.
- If there is a problem, the Status LED flashes fast amber. If this happens, call your IT department.
- Step 6** Observe the Status LED on the back; when the device connects to the Cisco cloud, the Status LED slowly flashes green.
- If there is a problem, the Status LED flashes amber and green, and the device did not reach the Cisco Cloud. If this happens, 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 device does not reach the Cisco cloud after about 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 Firepower device 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


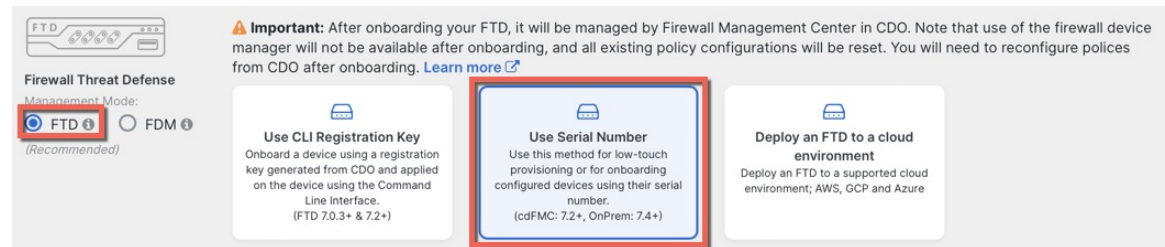
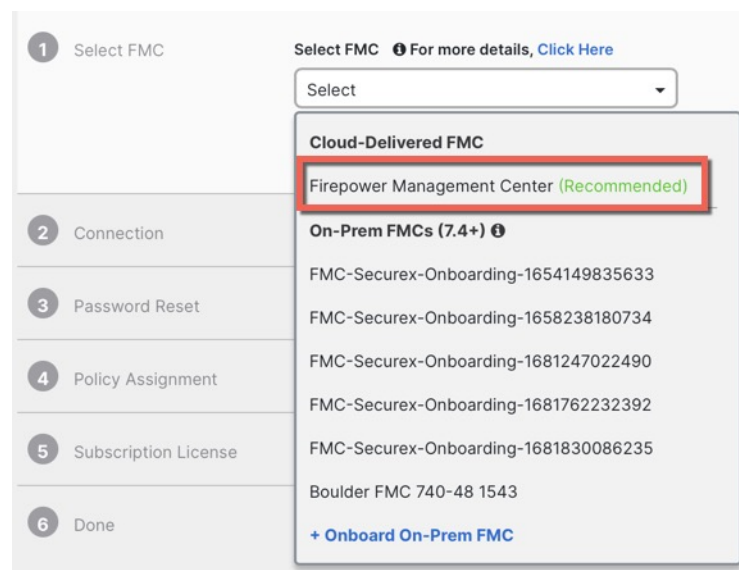
- Step 1** In the CDO navigation pane, click **Inventory**, then click the blue plus button () to **Onboard** a device.
- Step 2** Select the **FTD** tile.
- Step 3** Under **Management Mode**, be sure **FTD** is selected.
- At any point after selecting **FTD** as the management mode, you can click **Manage Smart License** to enroll in or modify the existing smart licenses available for your device. See [Obtain Licenses, on page 6](#) to see which licenses are available.
- Step 4** Select **Use Serial Number** as the onboarding method.

Figure 6: Use Serial Number



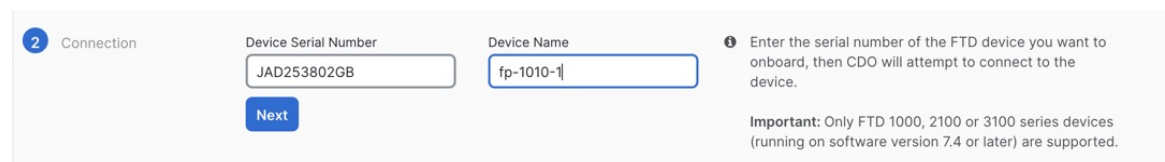
Step 5 In **Select FMC**, choose the **Cloud-Delivered FMC > Firewall Management Center** from the list, and click **Next**.

Figure 7: Select FMC



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

Figure 8: 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 9: Password Reset

3 Password Reset

1 Please review all the prerequisites for onboarding with a serial number. [Learn more](#)

2 Is this a new device that has never been logged into or configured for a manager?

Yes, this new device has never been logged into or configured for a manager

Enter a new password for devices that have never been configured for a manager.

Important: If you select this option and the device's default password has already been changed, onboarding fails.

New Password

Confirm Password

No, this device has been logged into and configured for a manager

Use this option if you already changed the password in the device CLI.

Important: If you select this option and the device's default password has not been changed, onboarding fails.

Password must:

- Be 8-128 characters
- Have at least one lower and one upper case letter
- Have at least one digit
- Have at least one special character.
- Not contain consecutive repeated letters

Next

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 10: Policy Assignment

4 Policy Assignment

Access Control Policy

Default Access Control Policy ▾

Next

Step 9

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

Figure 11: Subscription License

5 Subscription License

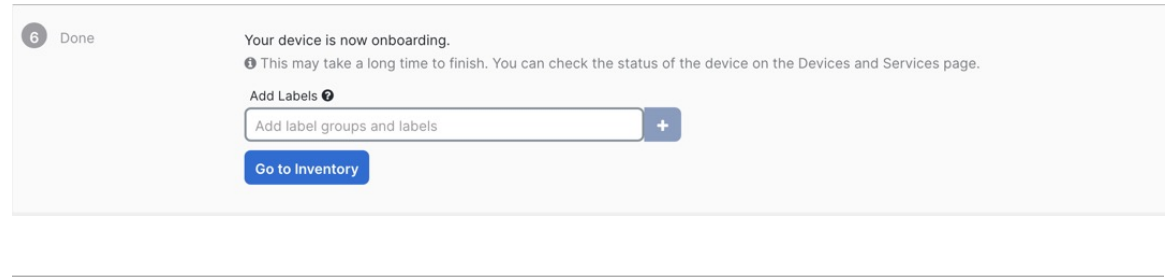
License Type	Includes
<input checked="" type="checkbox"/> Essentials	Base Firewall Capabilities
<input checked="" type="checkbox"/> Carrier (7.3+ FTDs only)	GTP/GPRS, Diameter, SCTP, M3UA
<input checked="" type="checkbox"/> IPS	Intrusion Policy
<input checked="" type="checkbox"/> Malware Defense	File Policy
<input checked="" type="checkbox"/> URL	URL Reputation
<input type="checkbox"/> RA VPN <input type="text" value="VPNOnly"/>	RA VPN

Enable subscription licenses. CDO will attempt to enable the selected licenses when the device is connected to CDO and registered with the supplied Smart License. Learn more about [Cisco Smart Accounts](#).

Next

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 12: 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.

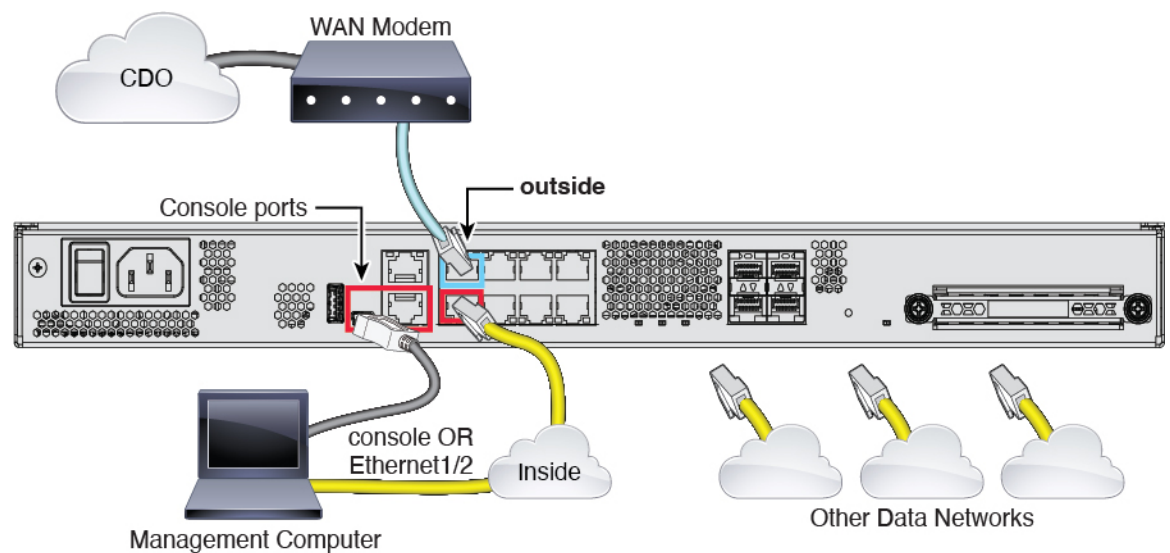
Deploy the Firewall With the Onboarding Wizard

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

Cable the Firewall

This topic describes how to connect the Firepower 1100 to your network so that it can be managed by CDO.

Figure 13: Cabling the Firepower 1100



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 initial 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 device. 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.



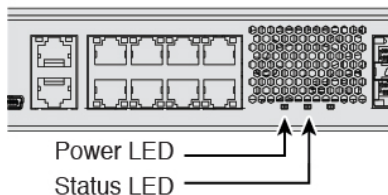
Note The first time you boot up the threat defense, initialization can take approximately 15 to 30 minutes.

Before you begin

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

Procedure

- Step 1** Attach the power cord to the device, and connect it to an electrical outlet.
- Step 2** Turn the power on using the standard rocker-type power on/off switch located on the rear of the chassis, adjacent to the power cord.
- Step 3** Check the Power LED on the back of the device; if it is solid green, the device is powered on.




- Step 4** Check the Status LED on the back of the device; 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.

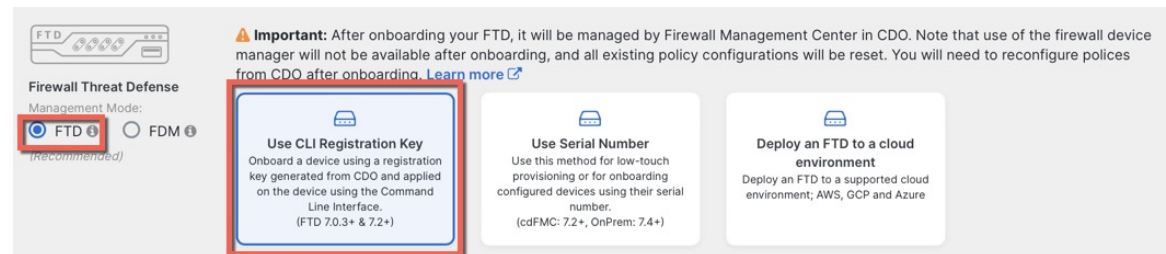
Step 2 Click the **FTD** tile.

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 6](#) to see which licenses are available.

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

Figure 14: Use CLI Registration Key



Step 5 Enter the **Device Name** and click **Next**.

Figure 15: Device Name

1 Device Name

Device Name

ftd1

Next

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 16: Access Control Policy

2 Policy Assignment

Access Control Policy

Default Access Control Policy ▾

Next

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 17: Subscription License

3 Subscription License

Please indicate if this FTD is physical or virtual:

Physical FTD Device

Virtual FTD Device

License Type	Includes
<input checked="" type="checkbox"/> Essentials	Base Firewall Capabilities
<input checked="" type="checkbox"/> Carrier (7.3+ FTDs only)	GTP/GPRS, Diameter, SCTP, M3UA
<input checked="" type="checkbox"/> IPS	Intrusion Policy
<input checked="" type="checkbox"/> Malware Defense	File Policy
<input checked="" type="checkbox"/> URL	URL Reputation
<input checked="" type="checkbox"/> RA VPN Premier ▾	RA VPN

Next

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 initial configuration of the threat defense.

Figure 18: CLI Registration Key

4 CLI Registration Key

1 Ensure the device's initial configuration is complete before trying to apply the registration key. [Learn more](#)

2 Copy the CLI Key below and paste it into the CLI of the FTD

```
configure manager add cisco-security-docs.app.us.cdo.cisco.com
BanyI2oaT0ew1JTpC0P2w3xEBnVVkfZv x7R7dwcM43JCMzwGY3ZzCfoFmZhw97my cisco-security-
docs.app.us.cdo.cisco.com
```

Next

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 19](#)—Copy this command at the threat defense CLI after you complete the startup script.

- [Perform Initial Configuration Using the Device Manager, on page 24](#)—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:

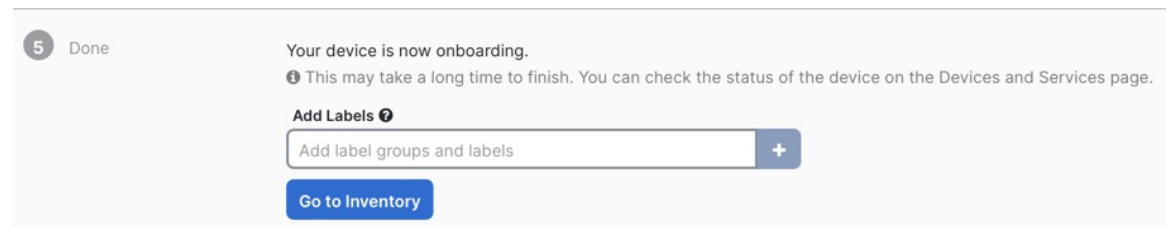
Figure 19: configure manager add command components

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

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 20: 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

Perform 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 management, 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 [Onboard a Device with the Onboarding Wizard, on page 17](#) 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 configuration 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 initial 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](#) 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 21: 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**.

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/>).

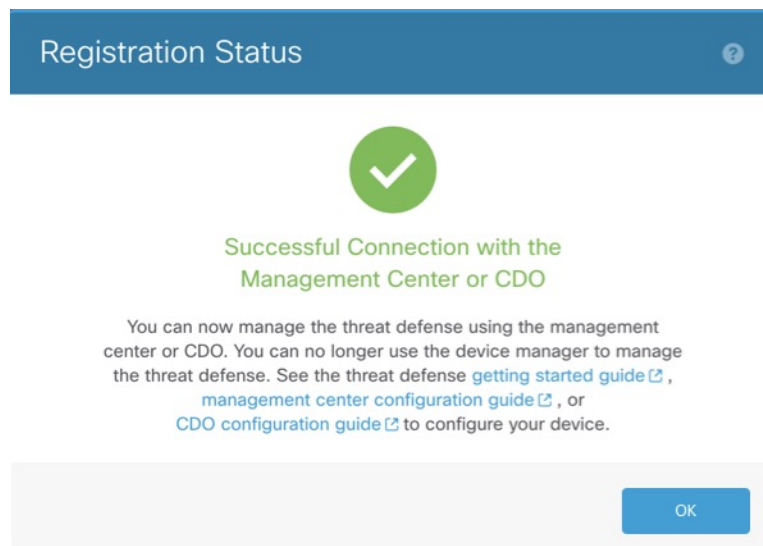
Step 11

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 23: 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.

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

The **General** tab appears.

Figure 25: General Tab

Edit Physical Interface

General IPv4 IPv6 Path Monitoring

Name:

Enabled
 Management Only

Description:

Mode:

Security Zone:

Interface ID:

MTU:

(64 - 9000)

Priority:
 (0 - 65535)

Propagate Security Group Tag:

NVE Only:

- Enter a **Name** up to 48 characters in length.
For example, name the interface **inside**.
- Check the **Enabled** check box.
- Leave the **Mode** set to **None**.
- 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.

- 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 26: IPv4 Tab

The screenshot shows the 'Edit Physical Interface' window with the 'IPv4' tab selected. The 'IP Type' dropdown is set to 'Use Static IP'. The 'IP Address' field contains '192.168.1.1/24'. Below the field, there is a small text example: '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 27: IPv6 Tab

The screenshot shows the 'Edit Physical Interface' window with the 'IPv6' tab selected. The 'Basic' sub-tab is active. The 'Enable IPv6' checkbox is unchecked. The 'Enforce EUI 64' checkbox is unchecked. The 'Link-Local address' field is empty. The 'Autoconfiguration' checkbox is checked. The 'Obtain Default Route' checkbox is unchecked.

f) Click **OK**.

- Step 4** Click **Edit** (✎) for the interface that you want to use for *outside*.
The **General** tab appears.

Figure 28: General Tab

Edit Physical Interface

General IPv4 IPv6 Path Monitoring Hardware

Name:

Enabled
 Management Only

Description:

Mode:

Security Zone:

Interface ID:

MTU:

(64 - 9000)

Priority:
 (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 5 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 29: DHCP Server

The screenshot shows the DHCP Server configuration page. The left sidebar contains a menu with 'DHCP Server' selected. The main area has tabs for 'Device', 'Routing', 'Interfaces', 'Inline Sets', 'DHCP', and 'VTEP'. The 'DHCP' tab is active, showing configuration fields for Ping Timeout (50), Lease Length (3600), and an unchecked 'Auto-Configuration' checkbox. Below these are fields for 'Interface', 'Domain Name', 'Primary DNS Server', 'Secondary DNS Server', 'Primary WINS Server', and 'Secondary WINS Server'. At the bottom, there are tabs for 'Server' and 'Advanced'. A table with columns 'Interface', 'Address Pool', and 'Enable DHCP Server' is shown, with 'No records to display' below it. A red box highlights the '+ Add' button in the top right corner of the table area.

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

Figure 30: Add Server

The screenshot shows the 'Add Server' dialog box. It has a title bar with 'Add Server' and a help icon. The 'Interface*' field is a dropdown menu with 'inside' selected. The 'Address Pool*' field is a text input with '10.9.7.9-10.9.7.25' entered, and '(2.2.2.10-2.2.2.20)' shown below it. There is a checked checkbox for 'Enable DHCP Server'. At the bottom, there are 'Cancel' and 'OK' buttons.

- **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**.

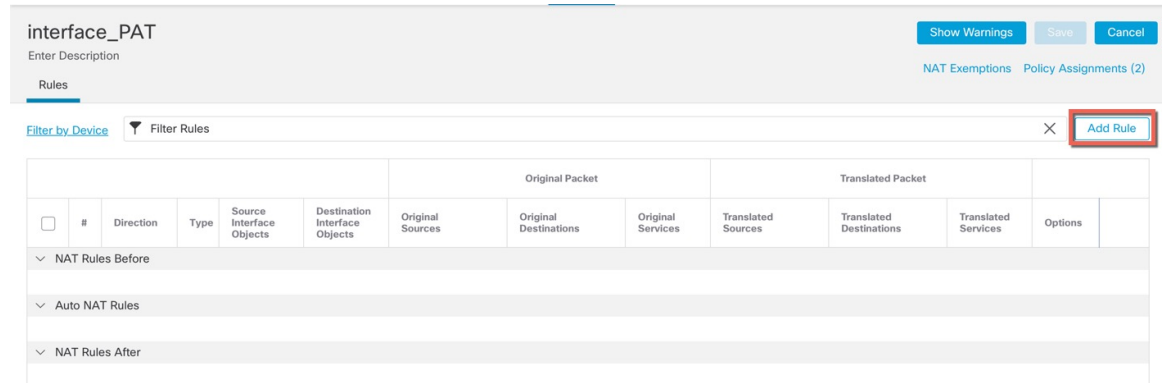
Figure 31: New Policy

The screenshot shows the 'New Policy' configuration interface. It includes the following elements:

- Name:** A text input field containing the text 'interface_PAT'.
- Description:** An empty text input field.
- Targeted Devices:** A section with the instruction 'Select devices to which you want to apply this policy.' and an unchecked checkbox.
- Available Devices:** A list of devices with a search box above it containing 'Search by name or value'. The list contains two entries: '10.10.0.6' and '10.10.0.7', with the second entry highlighted in blue.
- Selected Devices:** A list of devices that has been added to the policy, containing '10.10.0.6' and '10.10.0.7', each with a trash icon to its right.
- Buttons:** An 'Add to Policy' button is positioned between the 'Available Devices' and 'Selected Devices' lists. At the bottom right of the window are 'Cancel' and 'Save' buttons.

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

Figure 32: NAT Policy

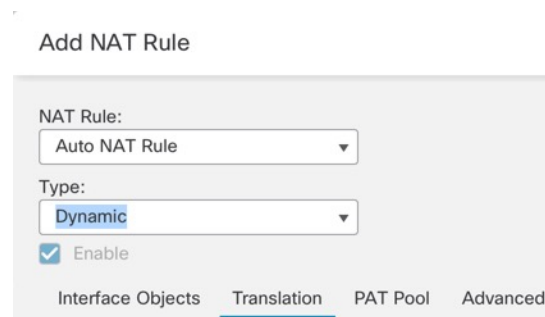


Step 3 Click **Add Rule**.

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

Step 4 Configure the basic rule options:

Figure 33: 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 34: Interface Objects

Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Dynamic

Enable

Interface Objects Translation PAT Pool Advanced

Available Interface Objects

- inside_zone
- 1 outside_zone** **2 Add to Destination**
- wfxAutomationZone

Source Interface Objects (0)

Destination Interface Objects (1)

- 3 outside_zone**

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

Figure 35: Translation

Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Dynamic

Enable

Interface Objects Translation PAT Pool Advanced

Original Packet

Original Source:* all-ipv4 +

Original Port: TCP

Translated Packet

Translated Source: Destination Interface IP

1 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 36: New Network Object

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 37: Add Rule

The screenshot shows the 'Create Rule' configuration page. At the top, there's a '1 Create Rule' header. Below it, the rule name is 'inside-to-outside'. The action is set to 'Allow', logging is 'OFF', and the time range is 'None'. The rule is currently enabled. There are several dropdown menus for 'Insert' (set to 'into Mandatory'), 'Intrusion Policy' (set to 'None'), 'Select Variable Set', and 'File Policy' (set to 'None'). Below these are tabs for 'Zones (2)', 'Networks', 'Ports', 'Applications', 'Users', 'URLs', 'Dynamic Attributes', and 'VLAN Tags'. The 'Zones (2)' tab is active, showing a search bar and a list of three zones: 'inside_zone (Routed Security Zone)', 'outside_zone (Routed Security Zone)', and 'wfxAutomationZone (Routed Security Zone)'. On the right, there are two sections: 'Selected Sources: 1' and 'Selected Destinations and Applications: 1'. The 'Selected Sources' section shows 'ZONE' with a dropdown arrow and '1 object' containing 'inside_zone'. The 'Selected Destinations and Applications' section shows 'ZONE' with a dropdown arrow and '1 object' containing 'outside_zone'. Each section has 'Collapse All' and 'Remove All' buttons.

- **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.

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; if your SSH host is located on the outside interface, you can only initiate a management connection directly to the outside interface.

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 **SSH Access**.
- 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.
 - **Available Zones/Interfaces**—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 Zones/Interfaces** list and click **Add**. You can also add loopback interfaces. 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 38: 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 39: Deploy All

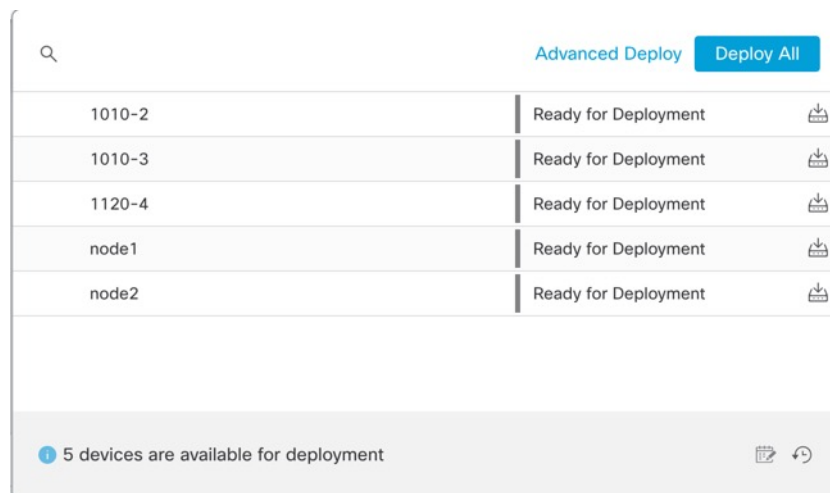


Figure 40: Advanced Deploy

Device	Modified by	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
<input checked="" type="checkbox"/> node1	System		FTD		May 23, 2022 6:49 PM		Ready for Deployment
<input type="checkbox"/> 1010-2	admin, System		FTD		May 23, 2022 7:09 PM		Ready for Deployment
<input type="checkbox"/> node2	System		FTD		May 23, 2022 6:49 PM		Ready for Deployment
<input type="checkbox"/> 1010-3	System		FTD		May 23, 2022 6:49 PM		Ready for Deployment
<input type="checkbox"/> 1120-4	System		FTD		May 23, 2022 6:49 PM		Ready for Deployment

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 41: Deployment Status

Deployment	Status	Message	Duration
1010-2	Success	Deployment to device successful.	2m 13s
1010-3	Success	Deployment to device successful.	2m 4s
1120-4	Success	Deployment to device successful.	1m 45s
node1	Success	Deployment to device successful.	1m 46s
node2	Success	Deployment to device successful.	1m 45s

Troubleshooting and Maintenance

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 Firepower 1000 ships with a USB A-to-B serial cable. 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#
```

Troubleshoot Management Connectivity on a Data Interface

When you use a data interface for manager access instead of using the dedicated Management interface, you must be careful about changing the interface and network settings for the threat defense in CDO so you do

not disrupt the connection. If you change the management interface type after you add the threat defense to CDO (from data to Management, or from Management to data), if the interfaces and network settings are not configured correctly, you can lose management connectivity.

This topic helps you troubleshoot the loss of management connectivity.

View management connection status

In CDO, check the management connection status on the **Devices > Device Management > Device > Management > Manager Access - Configuration Details > Connection Status** page.

At the threat defense CLI, enter the **sftunnel-status-brief** command to view the management connection status. You can also use **sftunnel-status** to view more complete information.

See the following sample output for a connection that is down; there is no peer channel "connected to" information, nor heartbeat information shown:

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

See the following sample output for a connection that is up, with peer channel and heartbeat information shown:

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

View the threat defense network information

At the threat defense CLI, view the Management and manager access data interface network settings:

show network

```
> show network
===== [ System Information ] =====
Hostname                : ftd-1
DNS Servers             : 208.67.220.220,208.67.222.222
Management port        : 8305
IPv4 Default route
  Gateway               : data-interfaces
IPv6 Default route
  Gateway               : data-interfaces

===== [ management0 ] =====
State                   : Enabled
Link                    : Up
Channels                : Management & Events
Mode                    : Non-Autonegotiation
```

```

MDI/MDIX                : Auto/MDIX
MTU                      : 1500
MAC Address              : 28:6F:7F:D3:CB:8D
-----[ IPv4 ]-----
Configuration            : Manual
Address                  : 10.99.10.4
Netmask                  : 255.255.255.0
Gateway                  : 10.99.10.1
-----[ IPv6 ]-----
Configuration            : Disabled

=====[ Proxy Information ]=====
State                    : Disabled
Authentication           : Disabled

=====[ System Information - Data Interfaces ]=====
DNS Servers              :
Interfaces                : Ethernet1/1

=====[ Ethernet1/1 ]=====
State                    : Enabled
Link                     : Up
Name                     : outside
MTU                      : 1500
MAC Address              : 28:6F:7F:D3:CB:8F
-----[ IPv4 ]-----
Configuration            : Manual
Address                  : 10.89.5.29
Netmask                  : 255.255.255.192
Gateway                  : 10.89.5.1
-----[ IPv6 ]-----
Configuration            : Disabled

```

Check that the threat defense registered with CDO

At the threat defense CLI, check that CDO registration was completed. Note that this command will not show the *current* status of the management connection.

show managers

```

> show managers
Type                    : Manager
Host                    : account1.app.us.cdo.cisco.com
Display name            : account1.app.us.cdo.cisco.com
Identifier               : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration             : Completed
Management type         : Configuration

```

Ping CDO

At the threat defense CLI, use the following command to ping CDO from the data interfaces:

ping cdo_hostname

At the threat defense CLI, use the following command to ping CDO from the Management interface, which should route over the backplane to the data interfaces:

ping system cdo_hostname

Capture packets on the threat defense internal interface

At the threat defense CLI, capture packets on the internal backplane interface (nlp_int_tap) to see if management packets are being sent:

capture *name* interface nlp_int_tap trace detail match ip any any

show capture *name* trace detail

Check the internal interface status, statistics, and packet count

At the threat defense CLI, see information about the internal backplane interface, nlp_int_tap:

show interace detail

```
> show interface detail
[...]
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
  (Full-duplex), (1000 Mbps)
  Input flow control is unsupported, output flow control is unsupported
  MAC address 0000.0100.0001, MTU 1500
  IP address 169.254.1.1, subnet mask 255.255.255.248
  37 packets input, 2822 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 pause input, 0 resume input
  0 L2 decode drops
  5 packets output, 370 bytes, 0 underruns
  0 pause output, 0 resume output
  0 output errors, 0 collisions, 0 interface resets
  0 late collisions, 0 deferred
  0 input reset drops, 0 output reset drops
  input queue (blocks free curr/low): hardware (0/0)
  output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
  37 packets input, 2304 bytes
  5 packets output, 300 bytes
  37 packets dropped
    1 minute input rate 0 pkts/sec,  0 bytes/sec
    1 minute output rate 0 pkts/sec,  0 bytes/sec
    1 minute drop rate, 0 pkts/sec
    5 minute input rate 0 pkts/sec,  0 bytes/sec
    5 minute output rate 0 pkts/sec,  0 bytes/sec
    5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
  Interface number is 14
  Interface config status is active
  Interface state is active
```

Check routing and NAT

At the threat defense CLI, check that the default route (S*) was added and that internal NAT rules exist for the Management interface (nlp_int_tap).

show route

```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```

E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF
Gateway of last resort is 10.89.5.1 to network 0.0.0.0

S*      0.0.0.0 0.0.0.0 [1/0] via 10.89.5.1, outside
C       10.89.5.0 255.255.255.192 is directly connected, outside
L       10.89.5.29 255.255.255.255 is directly connected, outside

>

```

show nat

```

> show nat

Auto NAT Policies (Section 2)
1 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_intf3 interface service
  tcp 8305 8305
  translate_hits = 0, untranslate_hits = 6
2 (nlp_int_tap) to (outside) source static nlp_server_0_ssh_intf3 interface service
  tcp ssh ssh
  translate_hits = 0, untranslate_hits = 73
3 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_ipv6_intf3 interface
  ipv6 service tcp 8305 8305
  translate_hits = 0, untranslate_hits = 0
4 (nlp_int_tap) to (outside) source dynamic nlp_client_0_intf3 interface
  translate_hits = 174, untranslate_hits = 0
5 (nlp_int_tap) to (outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
  translate_hits = 0, untranslate_hits = 0

>

```

Check other settings

See the following commands to check that all other settings are present. You can also see many of these commands on CDO's **Devices > Device Management > Device > Management > Manager Access - Configuration Details > CLI Output** page.

show running-config sftunnel

```

> show running-config sftunnel
sftunnel interface outside
sftunnel port 8305

```

show running-config ip-client

```

> show running-config ip-client
ip-client outside

```

show conn address fmc_ip

```

> show conn address 10.89.5.35
5 in use, 16 most used
Inspect Snort:
  preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap 10.89.5.29(169.254.1.2):51231 outside 10.89.5.35:8305, idle 0:00:04,
  bytes 86684, flags UxIO
TCP nlp_int_tap 10.89.5.29(169.254.1.2):8305 outside 10.89.5.35:52019, idle 0:00:02,

```

```
bytes 1630834, flags UIO
>
```

Check for a successful DDNS update

At the threat defense CLI, check for a successful DDNS update:

debug ddns

```
> debug ddns
DDNS update request = /v3/update?hostname=domain.example.org&myip=209.165.200.225
Successfully updated the DDNS sever with current IP addresses
DDNS: Another update completed, outstanding = 0
DDNS: IDB SB total = 0
```

If the update failed, use the **debug http** and **debug ssl** commands. For certificate validation failures, check that the root certificates are installed on the device:

show crypto ca certificates *trustpoint_name*

To check the DDNS operation:

show ddns update interface *fmc_access_ifc_name*

```
> show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name Update Destination
  RBD_DDNS not available

Last Update attempted on 04:11:58.083 UTC Thu Jun 11 2020
Status : Success
FQDN : domain.example.org
IP addresses : 209.165.200.225
```

Check CDO log files

See <https://cisco.com/go/fmc-reg-error>.

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 Device 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 41](#).

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.

