



Preconfiguring Firepower Managed Devices

You can preconfigure your Firepower devices at a *staging* location (a central location to preconfigure or stage multiple appliances) to be deployed at a *target* location (any location other than the staging location).

To preconfigure and deploy an appliance to a target location, perform the following steps:

- install the system on the device at the staging location
- optionally, register the device to a Management Center
- optionally, push any updates from the managing Management Center to the device
- optionally, unregister the device from the Management Center
- shut down and ship the appliance to the target location
- deploy the appliances in the target locations



Tip

Save all packing materials and include all reference material and power cords when repackaging the appliance.

Before You Begin

Before preconfiguring the appliance, collect the network settings, licenses, and other pertinent information for the staging location and the target location.



Tip

It can be helpful to create a spreadsheet to manage this information at the staging location and the target location.

During the initial setup, you configure your appliance with enough information to connect the appliance to the network and install the system. Optionally, you can connect a device to a Management Center to push any updates from the Management Center to the device. You can also enable other features that are not required for initial setup but can be useful to preconfigure.

Required Preconfiguration Information

At a minimum, you need the following information to preconfigure your appliance:

- the new password (initial setup requires changing the password)

- the hostname of the appliance
- the domain name of the appliance
- the IP management address of the appliance
- the network mask of the appliance at the target location
- the default gateway of the appliance at the target location
- the IP address of the DNS server at the staging location, or, if accessible, the target location
- the IP address of the NTP server at the staging location, or, if accessible, the target location
- the detection mode for the target location

Optional Preconfiguration Information

You can change some default configurations, such as:

- allow access to the LCD panel to configure Firepower devices
- set the time zone if you choose to manually set the time for your appliances
- set the remote storage location for automatic backups
- set the Lights-Out Management (LOM) IP address to enable LOM



Note

In some power cycle scenarios, the baseboard management controller (BMC) of a Firepower 7050 connected to the network via the management interface could lose the IP address assigned to it by the DHCP server. Because of this, Cisco recommends you configure the Firepower 7050 BMC with a static IP address. Alternately, you can disconnect the network cable and reconnect it, or remove and restore power to the device to force renegotiation of the link.

If you want to register a device to a Management Center, you need the following information:

- the name or IP address of the managed device
- the name of the management host (the Management Center)
- the registration key (a personally created unique alphanumeric key up to 37 characters in length)

Preconfiguring Time Management

Keep in mind the following considerations:

- Cisco recommends that you synchronize time to a physical NTP server. Do not synchronize managed devices to a virtual Management Center. Performance optimization on a virtual appliance can affect the real time clock.
- If the network at your staging location can access the DNS and NTP servers at the target location, use the IP addresses for the DNS and NTP servers at the target location. If not, use the staging location information and reset at the target location.
- Use the time zone for the target deployment if you set the time on the appliance to the manually instead of using NTP. See [Time Settings, page 5-7](#).

Installing the System

Use the installation procedures described in [Installing a Firepower Managed Device, page 4-1](#) and [Setting Up Firepower Managed Devices, page 5-1](#). When preconfiguring the system, keep the following in mind:

- If you allow access to a Firepower device's network settings using the LCD panel, you introduce a security risk where unauthorized changes can be made by physically accessing the device. See [Firepower Device LCD Panel Configuration, page 5-7](#).
- Pre-register a device using the host name or IP address of the Management Center in the target deployment. Note the registration key for later in completing the registration. See [Remote Management, page 5-7](#).
- If you change the default detection mode, be sure to notify the appropriate personnel at the target deployment. Configuring interfaces differently from the detection mode can cause the system to incorrectly assign interfaces. See [Detection Mode, page 5-8](#).
- If you need to configure Network Address Translation (NAT) for your device, provide the NAT ID of the device when registering the device using either the CLI on the device or the web interface on its managing Management Center. See [Registering a Firepower Device to a Management Center Using the CLI, page 5-4](#) and Working In NAT Environments in the *Firepower Management Center Configuration Guide*.
- Add licenses during the initial setup. If you do not add licenses at that time, any devices you register during initial setup are added to the Firepower Management Center as unlicensed; you must license each of them individually after the initial setup process is over. See *Firepower Management Center Installation Guide* for more information.

Registering a Device

Access: Admin

You can register a device to a Management Center to push policies and updates to the managed device if your Management Center is running a software version equal to or greater than the software version on the device.

**Note**

If you deploy the Management Center and its managed device in different target locations, you must delete the device from the Management Center before shutting down the appliances. See [Deleting Devices from a Management Center, page E-4](#).

To register a device to a Management Center:**Step 1**

On the device, configure remote management using the host name or IP address of the Management Center in the target deployment. Note the registration key for later use in completing the registration. See [Remote Management, page 5-7](#).

**Note**

You must configure remote management on the device before you can register the device to a Management Center.

What to Do Next

- On the Management Center, register the device using the registration information from your remote management configuration. See the *Firepower Management Center Installation Guide* for more information.

Preparing the Appliance for Shipment

To prepare the appliance for shipment, you must safely power down and repackage the appliance:

- If your managed device will not be used in the same configuration at the target location, you must delete the device from the Management Center, then power down and repackage the appliances. See [Deleting Devices from a Management Center, page E-4](#).
- To safely power down the appliance, see [Powering Down the Appliance, page E-5](#).
- To ensure that your appliance is safely prepared for shipping, see [Shipping Considerations, page E-5](#).


Deleting Devices from a Management Center

Access: Admin

Unless you deploy the Management Center and its managed device at the same target location, you must delete the device from the Management Center. This prevents the device from looking for the UUID of the original Management Center when you register the device to a different Management Center at the target location.

To delete a device from the Management Center:

Step 1 On the Management Center, Select **Devices > Device Management**.

Step 2 Next to the device you want to delete, click the delete icon ().

When prompted, confirm that you want to delete the device. Communication between the device and the Management Center is discontinued and the device is deleted from the Device Management page. If the device has a system policy that causes it to receive time from the Management Center via NTP, the device reverts to local time management.

After deleting the device from the Management Center, verify that the device is not remotely managed by the Management Center.

To verify that a Firepower device is not managed by a Management Center:

Step 1 On the Firepower device, you can use either the web interface or the CLI:


- On the web interface of the Firepower device, go to **System > Registration > Remote Management** and confirm that the Host list on the Remote Management screen is empty.
 - On the CLI of the Firepower device, run the command `show manager` and confirm that no host is displayed.
-

Deleting a License from a Management Center

Access: Admin

Use the following procedure if you need to delete a license for any reason. Keep in mind that, because Cisco generates licenses based on each Management Center's unique license key, you cannot delete a license from one Management Center and reuse it on a different Management Center. For more information, see See Licensing the Firepower System in the *Firepower Management Center Configuration Guide*.

To delete a license:

-
- Step 1** Select **Systems > Licenses**.
- Step 2** Next to the license you want to delete, click the delete icon ().
- Deleting a license removes the licensed capability from all devices using that license. For example, if your Protection license is valid and enabled for 100 managed devices, deleting the license removes protection capabilities from all 100 devices.
- Step 3** Confirm that you want to delete the license.
- The license is deleted.
-

Powering Down the Appliance

Access: Admin

Use the following procedures to power down the appliance safely before disconnecting the power supply.

To power down a Firepower device:

-
- Step 1** On the device, enter the following at the command line:
- ```
system shutdown
```
- The device shuts down safely.
- 

## Shipping Considerations

To prepare the appliance for shipment to the target location, you must safely power down and repackage the appliance. Keep in mind the following considerations:

- Use the original packaging to repack the appliance.
- Include all reference material and power cords with the appliance.
- Protect the NetMods and SFPs from damage caused by improper handling or undue pressure.
- Provide all setting and configuration information to the target location, including the new password and the detection mode.

# Troubleshooting the Appliance Preconfiguration

If your appliance is correctly preconfigured for target deployment, you can install and deploy the appliance without further configuration.

If you have difficulty logging into the appliance, the preconfiguration may have an error. Try the following troubleshooting procedures:

- Confirm that all power cables and communication cables are connected properly to the appliance.
- Confirm that you have the current password for your appliance. The initial setup at the staging location prompts you to change your password. See the configuration information provided by the staging location for the new password.
- Confirm that the network settings are correct. See [Initial Setup Page: Firepower Devices, page 5-5](#).
- Confirm that the correct communication ports are functioning properly. See the documentation for your firewall for information on managing firewall ports. See [Communication Ports Requirements, page 1-14](#) for required open ports.
- If you use a Network Address Translation (NAT) appliance in your deployment, confirm that NAT is configured correctly. See Working in NAT Environments in the *Firepower Management Center Configuration Guide*.

If you continue to experience difficulty, contact your IT department.