Cisco Firepower Management Center 750, 1500, 2000, 3500, and 4000 Getting Started Guide

Updated: April 6, 2020

This guide is organized as follows:

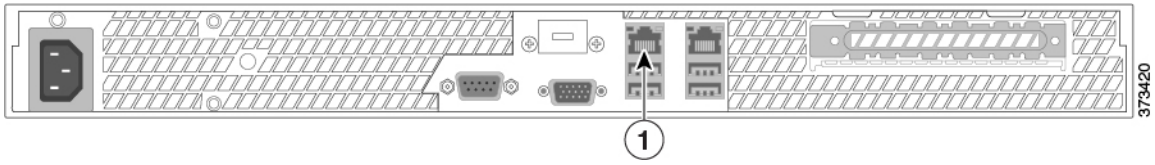
Package Contents

This section lists the items included with each model. Note that contents are subject to change, and your exact contents might contain additional or fewer items.

Chassis Models

- Firepower Management Center 750 (1U model). The following illustration of the rear of the chassis indicates the location of the management interface on a MC750.

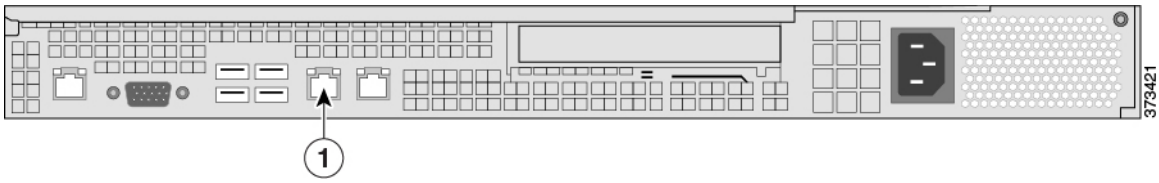
Figure 1 MC750 Chassis and Management Interface



1	Management interface		

- Firepower Management Center 1500 (1U model). The following illustration of the rear of the chassis indicates the location of the management interface on a MC1500.

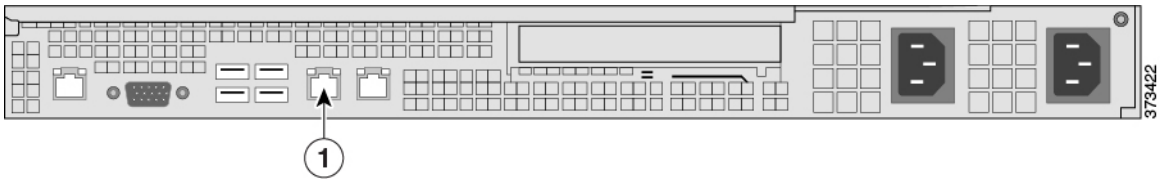
Figure 2 MC1500 Chassis and Management Interface



1	Management interface		

- Firepower Management Center 3500 (1U model). The following illustration of the rear of the chassis indicates the location of the management interface on a MC3500.

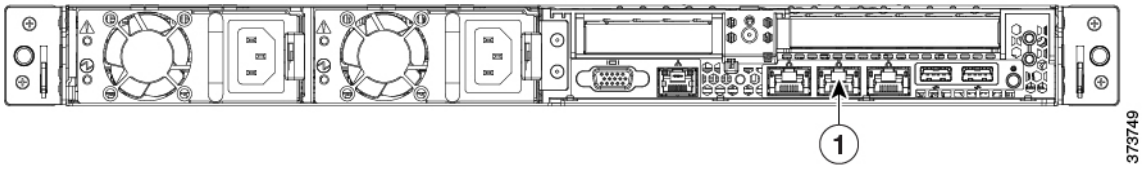
Figure 3 MC3500 Chassis and Management Interface



1	Management interface		

- Firepower Management Center 2000/4000 (1U model). The following illustration of the rear of the chassis indicates the location of the management interface.

Figure 4 MC2000 and MC4000



1	Management interface		

Included Items

- One power cord per power supply.
- One straight-through Cat 5e Ethernet cables per chassis.
- One rack-mounting kit per chassis.

License Requirements

You can license a variety of features to create an optimal Firepower System deployment for your organization. You use the Firepower Management Center to manage licenses for itself and the devices it manages. The license types offered by the Firepower System depend upon the type of device you want to manage:

Classic Licenses

For 7000 and 8000 Series, ASA FirePOWER, and NGIPSv devices, you must use Classic Licenses. Devices that use Classic Licenses are sometimes referred to as Classic devices.

If your FMC is using a Firepower Version previous to 6.5: Cisco recommends that you use the initial setup page to add the classic licenses your organization has purchased; see License Settings, page 15. If you do not add classic licenses during initial setup, any devices you register during initial setup are added to the Management Center as unlicensed; you must license each of them individually after the initial setup process is over. Note that if you are setting up a reimaged appliance and you kept your license settings as part of the restore process, this section of the initial setup page may be prepopulated.

If your FMC is using Firepower Version 6.5+: You must add classic licenses for managed devices after completing the Initial Configuration Wizard. You can assign licenses to managed devices when you register them to the Firepower Management Center, or after you have registered them to the Firepower Management Center.

Smart Licenses

For Firepower Threat Defense physical and virtual devices, you must use Smart Licenses.

Cisco Smart Licensing lets you purchase and manage a pool of licenses centrally. Unlike product authorization key (PAK) licenses, smart licenses are not tied to a specific serial number or license key. Smart licensing lets you assess your license usage and needs at a glance.

Refer to the *Firepower Management Center Configuration Guide* for information about Classic Licenses and Smart Licenses, the types of licenses for each class, and how to manage the licenses across your deployment.

Accessing the CLI or the Linux Shell on the FMC

Accessing the FMC CLI or the Linux shell requires a different sequence of steps depending on what Firepower version the FMC is running. Refer to this topic when you encounter instructions in this document to log into to the FMC CLI or Linux shell.

Caution: We strongly recommend that you do you do not use the Linux shell unless directed by TAC or explicit instructions in the user documentation.

Before You Begin:

Establish a direct physical connection with the FMC using a keyboard and monitor or establish an SSH session with the FMC's managment interface.

Procedure

1. Log into the FMC using the credentials for the CLI **admin** user.

   Determine your next action depending on the Firepower version in use:

   - If your FMC is running Firepower Version 5.4 – 6.2.x, this gives you direct access to the Linux shell.
   - If your FMC is running Firepower Version 6.3.x or 6.4.x and the FMC CLI is not enabled, this gives you direct access to the Linux shell.
   - If your FMC is running Firepower Version 6.3.x or 6.4.x and the FMC CLI is enabled, this gives you access to the FMC CLI. To access the Linux shell, continue with Step 2.

- If your FMC is running Firepower Version 6.5+, this gives you access to the FMC CLI. To access the Linux shell, continue with Step 2.

2. To access the Linux shell form the FMC CLI, enter the **expert** command.

Installation and Initial Setup for Versions 6.5+

Note: Firepower Versions 6.5+ are not supported on FMC models 750, 1500, and 3500.

The first time you log into the FMC running Versions 6.5+, an Initial Configuration Wizard guides you through configuring the new appliance to communicate on your trusted management network. The wizard presents a streamlined initial configuration process and automatically establishes some weekly maintenance activities to keep your system up-to-date and your data backed up.

The FMC management interface is pre-configured to accept an IPv4 address assigned by the Dynamic Host Configuration Protocol (DHCP). If the FMC fails to obtain a DHCP lease, the management interface uses a fallback IPv4 address of 192.168.45.45.

Note: If you are connecting to an FMC for the first time after performing a System Restore and you chose to retain license and network settings, the management interface IP address is the same as it was before you performed the System Restore. Proceed directly to Firepower Management Center Initial Configuration Wizard, page 7.

To install and set up an FMC running Versions 6.5+:

1. Install the appliance as described in Install the Appliance, page 4.
2. To perform the initial setup you have one of two choices:
   - If your network does not use DHCP and your PC cannot reach the fallback address (or the address retained in a System Restore), we recommend you perform the initial setup by connecting a computer directly to the FMC's physical management interface as described in Access the Firepower Management Center Using the Management Interface, page 5.
   - If your local DHCP will assign an address to the FMC, use a keyboard and monitor to set up the appliance; see Access the Firepower Management Center Using a Keyboard and Monitor, page 6.

Install the Appliance

These instructions are an abbreviated version of the steps to physically install the appliance. For detailed instructions, see the *Cisco Firepower Management Center 750, 1500, 2000, 3500, and 4000 Hardware Installation Guide*.

Procedure

1. Mount the appliance in your rack using the mounting kit and its supplied instructions.
2. Attach power cords to both power supplies and plug them into separate power sources.

   If you do not connect both power supplies, an amber warning indicator lights on the chassis front panel and the FMC web interface displays a health alert.
3. Turn on the appliance by pressing the power switch located on the front panel.

   After you press the power switch the appliance may turn on briefly and then appear to shut down with the exception of the amber power indicator light on the chassis front panel. This is normal; pressing the power button again causes the appliance to power up with the power indicator light green.

What to Do Next

- The FMC management interface is pre-configured to accept an IPv4 address assigned by DHCP, but failing to obtain a DHCP lease, the management interface uses a fallback IPv4 address of192.168.45.45. Or, if you are connecting to an FMC for the first time after performing a System Restore and you chose to retain license and network settings, the IP address is the same as it was before you performed the System Restore. Ensure that you have established one of the following methods of accessing the appliance before proceeding:
  - If your network does not use DHCP and your PC cannot reach the fallback address (or the address retained in a System Restore), we recommend you perform the initial setup by connecting a computer directly to the FMC's physical management interface as described in Access the Firepower Management Center Using the Management Interface, page 5.
  - If your local DHCP will assign an address to the FMC, use a keyboard and monitor to set up the appliance; see Access the Firepower Management Center Using a Keyboard and Monitor, page 6.
- Perform the initial configuration process; see Firepower Management Center Initial Configuration Wizard, page 7.
- Optionally use the Smart License pop-up dialog to configure Smart Licensing. See Smart Licensing Dialog, page 9.
- Once you complete the Initial setup process, you can optionally configure the FMC for Serial or Serial over LAN (SOL) access; see Redirecting Console Output, page 19 and Setting Up Lights-Out Management, page 20.

After you complete setup, you will use the Firepower Management Center's web interface to perform most management and analysis tasks for your deployment. For more information, see Administration Recommendations, page 17.

Access the Firepower Management Center Using the Management Interface

The FMC management interface is pre-configured to accept an IPv4 address assigned by DHCP, but in scenarios where no DHCP is involved, the management interface uses the IPv4 address 192.168.45.45. Or, if you are connecting to an FMC for the first time after performing a System Restore and you chose to retain license and network settings, the IP address is the same as it was before you performed the System Restore.

Before You Begin:

- Configure a local computer, which must not be connected to the Internet, with the following network settings:
  - IP address: 192.168.45.2
  - netmask: 255.255.255.0
  - default gateway: 192.168.45.1
- Determine the IP address assigned to the management interface of the FMC:
  - If you are connecting to an FMC for the first time after performing a System Restore (see Restoring a Firepower Management Center to Factory Defaults, page 22) and you chose to retain license and network settings, the IP address is the same as it was before you performed the System Restore.
  - Otherwise the FMC management interface IP address is 192.168.45.45.

Procedure

1. Using the supplied Ethernet cable, connect the network interface on the preconfigured computer directly to the management interface on the appliance.

   Confirm that the link LED is on for both the network interface on the local computer and the management interface on the appliance.

2. Use a web browser to navigate to the appliance's IP address:

   ```
   https://<Management IP Address>
   ```

   The login page appears.

3. Log in to the web interface using `admin` as the username and `Admin123` as the password. (Note the password is case-sensitive.)

What to Do Next

- Complete the setup process using the procedures in Firepower Management Center Initial Configuration Wizard, page 7.

Access the Firepower Management Center Using a Keyboard and Monitor

You can connect a USB keyboard and VGA monitor to the appliance, which is useful for rack-mounted appliances connected to a keyboard, video, and mouse (KVM) switch. The FMC management interface is pre-configured to accept an IPv4 address assigned by DHCP, but failing to obtain a DHCP lease, the management interface uses a fallback IPv4 address of192.168.45.45. If your network does not use DHCP and your PC cannot reach that address, we recommend you perform the initial setup by connecting to the FMC directly as described in Access the Firepower Management Center Using the Management Interface, page 5.

Before You Begin:

Determine the IP address assigned to the management interface of the FMC:

- If you are setting up a new FMC for the first time, check with your network administrator to determine the IP address that DHCP will assign to the FMC's MAC address when you connect it to the local network. (You can find the MAC address on a label or pullout card on the appliance.)
- If no DHCP is present, or if the DHCP has no free addresses in its pool, the FMC management interface uses the IP address 192.168.45.45. In this case if your PC cannot reach that address we recommend you perform the initial setup by connecting to the FMC directly as described in Access the Firepower Management Center Using the Management Interface, page 5.
- If you are connecting to an FMC for the first time after performing a System Restore (see Restoring a Firepower Management Center to Factory Defaults, page 22) and you chose to retain license and network settings, the IP address is the same as it was before you performed the System Restore.

Procedure

1. Using the supplied Ethernet cable, connect the management interface on the back of the FMC to a protected management network.
2. Use a web browser to navigate to the FMC web interface login page:

   ```
   https://<Management IP Address>
   ```

   The login page appears.

3. Log into the web interface using `admin` as the username and `Admin123` as the password. Note that the password is case-sensitive.

What to Do Next

- Complete the setup process using the procedures in Firepower Management Center Initial Configuration Wizard, page 7.

Firepower Management Center Initial Configuration Wizard

When you log into the FMC web interface for the first time on a new appliance, or an appliance on which you have just performed a System Restore, the FMC presents an Initial Configuration Wizard to enable you to quickly and easily configure basic settings for the appliance. This wizard consists of three screens and one pop-up dialog:

- The first screen forces you to change the password for the `admin` user from the default value of `Admin123`.
- The second screen presents the End User License Agreement (EULA), which you are required to accept before using the appliance.
- The third screen allows you to change network settings for the appliance management interface. This page is pre-populated with current settings, which you may change.
- After you have completed the three wizard screens, a pop-up dialog appears that offers you the opportunity to (optionally) quickly and easily set up Smart Licensing.

When you have completed the Initial Configuration Wizard and completed or dismissed the Smart Licensing dialog, the system displays the device management page, described in "Device Management Basics" in the *Firepower Management Center Configuration Guide* for your version.

Change Password

To ensure system security and privacy, the first time you log in to the FMC you are required to change the `admin` password. When the Change Password wizard screen appears, you have two options:

- Enter a new password in the New Password and Confirm Password text boxes. The password must comply with the criteria listed in the dialog.
- Click the Generate Password button to have the system create a password for you which complies with the listed criteria. (Generated passwords are non-mnemonic; take careful note of the password if you choose this option.)

Check the **Show password** checkbox to see the password while using this screen. The wizard displays a list of criteria the new password must satisfy; a green check mark appears next to each criterion that has been met. If the new password does not meet all the listed criteria the wizard rejects the password and prevents you from proceeding to the next page.

The FMC compares your password against a password cracking dictionary that checks not only for many English dictionary words but also for other character strings that could be easily cracked with common password hacking techniques. For example, the initial configuration script may reject passwords such as "abcdefg" or "passw0rd".

Note: On completion of the initial configuration process the system sets the passwords for the two **admin** accounts (one for web access and the other for CLI access) to the same value, complying with the strong password requirements described in the *Firepower Management Center Configuration Guide* for your version. If you change the password for either **admin** account thereafter, they will no longer be the same, and the strong password requirement can be removed from the web interface **admin** account.

Note: Once you click **Next** on the Change Password screen and the wizard has accepted the new `admin` password, that password is in effect for both the web interface and CLI `admin` accounts even if you do not complete the remaining wizard activities.

End User License Agreement (EULA)

Before using the Firepower Management Center, you must accept the EULA displayed on the second Initial Configuration Wizard screen. Read the EULA and click **Accept** to proceed. If you click **Decline** the wizard logs you out of the FMC.

Change Network Settings

The final Initial Configuration Wizard screen gives you the opportunity to change the network settings the FMC uses for network communications through its management interface (eth0). If you are logging in for the first time after performing a System Restore in which you chose to retain network and license settings, the wizard is pre-populated with the same values the FMC used before the System Restore.

The wizard performs validation on the values you enter on this screen to confirm the following:

- syntactical correctness
- compatibility of the entered values (for instance, compatible IP address and gateway, or DNS provided when NTP servers are specified using FQDNs)
- network connectivity between the FMC and the DNS and NTP servers

The wizard displays the results of these tests in real-time on the screen, permitting you to make corrections and test the viability of your configuration before clicking **Finish** at the bottom of the screen. The NTP and DNS connectivity tests are not blocking; you can click **Finish** before the wizard completes the connectivity tests. If the system reports a connectivity problem after you click **Finish**, you cannot change the settings in the wizard, but you can configure these connections using the FMC web interface after completing the initial setup.

The system does not perform connectivity testing if you enter configuration values that would result in cutting off the existing connection between the FMC and the browser. In this case the wizard displays no connectivity status information for DNS or NTP.

You can set values for the following fields:

Fully Qualified Domain Name

You must provide a FQDN. You can do one of the following:

- accept the displayed value, if one is shown
- enter a fully qualified domain name (syntax `<hostname>.<domain>)` or host name

Boot Protocol for IPv4 Configuration

Choose one of the following methods of IP address assignment from the drop-down labeled **Configure IPv4**:

- **Using DHCP**
- **Using Static/Manual**

IPv4 Address

This field is required. You can accept the displayed value, if one is shown, or enter a new value. Use dotted decimal form (for example, 192.168.45.45).

Network Mask

This field is required. You can accept the displayed value, if one is shown, or enter a new value. Use dotted decimal form (for example, 255.255.0.0).

Gateway

You can accept the displayed gateway value if one is shown, or enter a new default gateway. Use dotted decimal form (for example, 192.168.0.1).

DNS Group

Choose an optional Domain Name Server group for the FMC. You can:

- Accept the default value, **Cisco Umbrella DNS**.

- Select **Custom DNS Servers** from the drop-down list, and enter IPv4 addresses for the **Primary DNS** and **Secondary DNS**.
- Configure no DNS Server by selecting **Custom DNS Servers** from the drop-down list and leaving the **Primary DNS** and **Secondary DNS** fields blank.

NTP Group Servers

You must use an NTP Server to ensure proper synchronization between the FMC and its managed devices. Choose one of the following from the drop-down list:

- **Default NTP Servers** By default the system uses `0.sourcefire.pool.ntp.org` as the primary NTP server, and `1.sourcefire.pool.ntp.org` as the secondary NTP server.
- **Custom NTP Servers** Enter the FQDN or IP addresses of one or two NTP servers reachable from your network.

Smart Licensing Dialog

After you click **Finish** on the Change Network Settings screen of the Initial Configuration Wizard, the system displays a pop-up that offers you the opportunity to quickly and easily set up Smart Licensing. Using this dialog is optional; if your FMC will be managing Firepower Threat Defense devices and you are familiar with Smart Licensing, use this dialog. Otherwise dismiss this dialog and refer to "Licensing the Firepower System" in the *Firepower Management Center Configuration Guide* for your version.

Automatic Initial Configuration

After you have completed the Initial Configuration Wizard the FMC automatically configures weekly maintenance activities to keep your system up-to-date and your data backed up:

The tasks are scheduled in UTC, which means that when they occur locally depends on the date and your specific location. Also, because tasks are schedule in UTC, they do not adjust for Daylight Saving Time, summer time, or any such seasonal adjustments that you may observe in your location. If you are affected, scheduled tasks occur one hour "later" in the summer than in the winter, according to local time.

Note: We strongly recommend you review the auto-scheduled configurations and adjust them if necessary.

- Weekly GeoDB Updates

  The FMC automatically schedules GeoDB updates to occur each week at the same randomly selected time. You can observe the status of this task using the web interface Message Center. If the system fails to configure the update and your FMC has internet access, we recommend you configure regular GeoDB updates as described in the *Firepower Management Center Configuration Guide* for your software version.

- Weekly FMC Software Updates

  The FMC automatically schedules a weekly task to download the latest software for the FMC and its managed devices. This task is scheduled to occur between 2 and 3 AM UTC on Sunday mornings; depending on the date and your specific location this can occur anywhere from Saturday afternoon to Sunday afternoon local time. You can observe the status of this task using the web interface Message Center. If the task scheduling fails and your FMC has internet access, we recommend you schedule a recurring task for downloading software updates as described in the *Firepower Management Center Configuration Guide* for your version.

  This task only downloads software patch and hotfix updates for the version your appliances are currently running; it is your responsibility to install any updates this task downloads. See the Cisco *Firepower Management Center Upgrade Guide* for more information.

- Weekly FMC Configuration Backup

The FMC automatically schedules a weekly task to perform a locally-stored configuration-only backup at 2 AM UTC on Monday mornings; depending on the date and your specific location this can occur anywhere from Saturday afternoon to Sunday afternoon local time. You can observe the status of this task using the web interface Message Center. If the task scheduling fails, we recommend you schedule a recurring task to perform backups as described in the *Firepower Management Center Configuration Guide* for your version.

- Vulnerability Database Update

  In Versions 6.6+, the FMC downloads and installs the latest vulnerability database (VDB) update from the Cisco support site. This is a one-time operation. You can observe the status of this update using the web interface Message Center. To keep your system up to date, if your FMC has internet access, we recommend you schedule tasks to perform automatic recurring VDB update downloads and installations as described in the *Firepower Management Center Configuration Guide* for your version.

- Daily Intrusion Rule Update

  In Versions 6.6+, the FMC configures a daily automatic intrusion rule update from the Cisco support site. The FMC deploys automatic intrusion rule updates to affected managed devices when it next deploys affected policies. You can observe the status of this update using the web interface Message Center. You can see the configuration for this task in the web interface under **System > Updates > Rule Updates**. If configuring the update fails and your FMC has internet access, we recommend you configure regular intrusion rule updates as described in the *Firepower Management Center Configuration Guide* for your version.

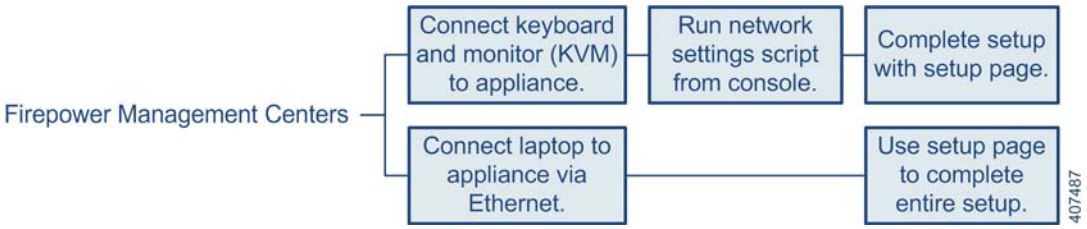
Installation and Initial Setup for Versions 5.4 – 6.4.x

Firepower Versions 5.4 – 6.4.x are supported on all FMC models addressed in this document: 750, 1500, 2000, 3500 and 4000.

When you install an appliance, make sure that you can access the appliance's console for initial setup. You can access the console for initial setup using a keyboard and monitor with KVM, or using an Ethernet connection to the management interface.

The first time you log into the FMC web interface, the initial administration page provides you with the ability to configure the new appliance to communicate on your trusted management network. You must also perform initial administrative-level tasks such as changing the administrator password, accepting the end user license agreement (EULA), setting the time, and scheduling updates. The options you choose during setup and registration determine the default interfaces, inline sets, zones, and policies that the system creates and applies to managed devices.

You can perform this initial setup process accessing the FMC either using a laptop directly connected to the appliance, or using an Ethernet connection through your trusted local management network. The following diagram illustrates the choices you can make when setting up FMC's running Firepower Versions 5.4 – 6.4.x:



Note: If you are deploying multiple appliances, set up your devices first, then their managing Firepower Management Center. The initial setup process for a device allows you to preregister it to a Management Center; the setup process for a Management Center allows you to add and license preregistered managed devices.

Note: If you are setting up an appliance after restoring it to factory defaults (see Restoring a Firepower Management Center to Factory Defaults, page 22) and you did not delete the appliance's license and network settings, you can use a computer on your management network to browse directly to the appliance's web interface to perform the setup. Skip to Initial Setup Page: Management Centers, page 13.

To install and set up an FMC running Versions 5.4 – 6.4.x:

1. Install the appliance as described in Install the Appliance, page 4.
2. Before connecting the FMC to your network you must change the FMC eth0 IP address to match your network and perform the initial setup; you have one of two choices:
   - Access the FMC using the VGA/keyboard connection to set the eth0 IP address before performing the initial setup; see Access the Firepower Management Center Using a Keyboard and Monitor, page 6.

     Then access the FMC with a web browser to perform the initial configuration process; see Initial Setup Page: Management Centers, page 13.
   - Access the FMC using an ethernet connection directly from the eth0 interface to a local computer; see Access the Firepower Management Center Using the Management Interface, page 5.

     Then access the FMC with a web browser to perform the initial configuration and set the eth0 IP address as a part of that process; see Initial Setup Page: Management Centers, page 13.

Install the Appliance

These instructions are an abbreviated version of the steps to physically install the appliance. For detailed instructions, see the *Cisco Firepower Management Center 1000, 2500, and 4500 Hardware Installation Guide*.

Procedure

1. Mount the appliance in your rack using the mounting kit and its supplied instructions.
2. Attach the power cord to the appliance and plug into a power source.

   If your appliance has redundant power supplies, attach power cords to both power supplies and plug them into separate power sources.
3. Turn on the appliance.

What to Do Next

- If you are connecting a computer directly to the appliance's physical management interface to set up the appliance, continue to Management Center Setup Using the Management Interface, page 11.
- If you are using a keyboard and monitor to set up the appliance, continue to Management Center Setup Using a Keyboard and Monitor (KVM), page 12.

Management Center Setup Using the Management Interface

Procedure

1. Configure a local computer, which must not be connected to the internet, with the following network settings:
   - IP address: 192.168.45.2
   - netmask: 255.255.255.0
   - default gateway: 192.168.45.1

(The FMC management interface is preconfigured with a default IPv4 address. However, you can reconfigure the management interface with an IPv6 address as part of the setup process.)

2. Using the supplied Ethernet cable, connect the network interface on the preconfigured computer directly to the management interface on the appliance.

   Confirm that the link LED is on for both the network interface on the local computer and the management interface on the appliance.

3. Use a web browser to navigate to the appliance's default IP address:

   ```
   https:// 192.168.45.45
   ```

   The login page appears.

4. Log in using `admin` as the username and `Admin123` as the password.

What to Do Next

- Complete the setup process using the procedures in Initial Setup Page: Management Centers, page 13.

Management Center Setup Using a Keyboard and Monitor (KVM)

You can connect a USB keyboard and VGA monitor to the appliance, which is useful for rack-mounted appliances connected to a keyboard, video, and mouse (KVM) switch.

Before You Begin

Be sure you have, at minimum, the information needed to allow the appliance to communicate on your management network:

- An IPv4 or IPv6 management IP address
- A netmask or prefix length
- A default gateway

Procedure

1. Using the supplied Ethernet cable, connect the management interface on the back of the appliance to a protected management network.
2. Connect the monitor to the VGA port and the keyboard to one of the USB ports.
3. Access the Linux shell on the FMC using using `admin` as the username and `Admin123` as the password. (Note that the password is case-sensitive.) Use the steps appropriate to your Firepower version; see Accessing the CLI or the Linux Shell on the FMC, page 3.
4. Run the following script:

   ```
   sudo /usr/local/sf/bin/configure-network
   ```

   The following prompt (appended with the current value) appears:

   ```
   Management IP address?
   ```

5. Enter the IP address you want to assign to the management interface or press Enter to accept the current value. For example:

   ```
   10.2.2.20
   ```

   The following prompt (appended with the current value) appears:

   ```
   Management netmask?
   ```

6. Enter the netmask for the interface's IP address or press Enter to accept the current value. For example:

```
255.255.255.0
```

The following prompt (appended with the current value) appears:

```
Management gateway?
```

7. Enter the gateway for the interface's IP address or press Enter to accept the current value. For example:

```
10.2.1.1
```

The following prompt appears:

```
Are these settings correct: (y or n)?
```

8. If the settings are correct, type y and press Enter to accept the settings and continue.

   If the settings are incorrect, type n and press Enter. You are prompted to enter the information again.

9. After you have accepted the settings, log out of the shell.

What to Do Next

- Complete the setup process using the procedures in Initial Setup Page: Management Centers, page 13.

Initial Setup Page: Management Centers

For all Management Centers, you must complete the setup process by logging into the Management Center's web interface and specifying initial configuration options on a setup page. You must change the administrator password, specify network settings if you haven't already, and accept the EULA.

In Versions 5.4.x, the setup process also allows you to register and license devices. Before you can register a device, you must complete the setup process on the device itself, as well as add the Management Center as a remote manager, or the registration will fail.

Procedure

1. Direct your browser to `https://`*`mgmt_ip`*`/`, where *`mgmt_ip`* is the IP address of the Management Center's management interface:
   - For a Management Center connected to a computer with an Ethernet cable, direct the browser on that computer to the default management interface IPv4 address: `https://192.168.45.45/`.
   - For a Management Center where network settings are already configured, use a computer on your management network to browse to the IP address of the Management Center's management interface.
2. Log in using `admin` as the username and `Admin123` as the password.

   See the following sections for information on completing the setup:
   - Change Password, page 14
   - Network Settings, page 14
   - Time Settings, page 15
   - Recurring Rule Update Imports, page 15
   - Recurring Geolocation Updates, page 15
   - Automatic Backups, page 15
   - License Settings, page 15
   - Device Registration, page 16
   - End User License Agreement, page 17

3. When you are finished, click **Apply**.

   The Management Center is configured according to your selections. You are logged into the web interface as the `admin` user, which has the Administrator role.

   Note: If you connected directly to the device using an Ethernet cable, disconnect the computer and connect the Management Center's management interface to the management network. Use a browser on a computer on the management network to access the Management Center at the IP address or host name that you just configured, and complete the rest of the procedures in this guide.

4. Confirm that the initial setup was successful:
   - For versions previous to 6.0, use the Task Status page (**System > Monitoring > Task Status**) to verify that the initial setup was successful.

     The page auto-refreshes every ten seconds. Monitor the page until it lists a status of **Completed** for the initial device registration and policy apply tasks. If, as part of setup, you configured an intrusion rule or geolocation update, you can also monitor those tasks.
   - For versions 6.0+, click the System Status icon and view the Tasks tab in the Message Center.

   The Management Center is ready to use. See the *Firepower Management Center Configuration Guide* for more information on configuring your deployment.

What to Do Next

- Continue with Administration Recommendations, page 17.

Setup Options

Change Password

You must change the password for the `admin` account. This account has Administrator privileges and cannot be deleted.

Cisco recommends that you use a strong password that is at least eight alphanumeric characters of mixed case and includes at least one numeric character. Avoid using words that appear in a dictionary.

Note: The admin accounts for accessing a Firepower Management Center using the shell versus accessing a Firepower Management Center using the web interface are not the same, and may use different passwords.

Network Settings

A Management Center's network settings allow it to communicate on your management network. If you already configured the network settings, this section of the page may be prepopulated.

The Firepower System provides a dual stack implementation for both IPv4 and IPv6 management environments. You must specify the management network protocol (**IPv4**, **IPv6**, or **Both**). Depending on your choice, the setup page displays various fields where you must set the IPv4 or IPv6 management IP address, netmask or prefix length, and default gateway:

- For IPv4, you must set the address and netmask in dotted decimal form (for example: a netmask of 255.255.0.0).
- For IPv6 networks, you can select the **Assign the IPv6 address using router autoconfiguration** check box to automatically assign IPv6 network settings. Otherwise, you must set the address in colon-separated hexadecimal form and the number of bits in the prefix (for example: a prefix length of 112).

You can also specify up to three DNS servers, as well as the host name and domain for the device.

Time Settings

You can set the time for a Management Center either manually or via network time protocol (NTP) from an NTP server.

You can also specify the time zone used on the local web interface for the `admin` account. Click the current time zone to change it using a pop-up window.

Recurring Rule Update Imports

As new vulnerabilities become known, the Cisco Talos Intelligence Group releases intrusion rule updates. Rule updates provide new and updated intrusion rules and preprocessor rules, modified states for existing rules, and modified default intrusion policy settings. Rule updates may also delete rules and provide new rule categories and system variables.

If you plan to perform intrusion detection and prevention in your deployment, Cisco recommends that you **Enable Recurring Rule Update Imports from the Support Site**.

You can specify the **Import Frequency**, as well as configure the system to perform an intrusion **Policy Reapply** after each rule update. To perform a rule update as part of the initial configuration process, select **Install Now**.

Rule updates may contain new binaries. Make sure your process for downloading and installing rule updates complies with your security policies. In addition, rule updates may be large, so make sure to import rules during periods of low network use.

Recurring Geolocation Updates

Firepower Management Centers can display geographical information about the routed IP addresses associated with events generated by the system, as well as monitor geolocation statistics in the dashboard and Context Explorer.

The Management Center's geolocation database (GeoDB) contains information such as an IP address's associated Internet service provider (ISP), connection type, proxy information, and exact location. Enabling regular GeoDB updates ensures that the system uses up-to-date geolocation information. If you plan to perform geolocation-related analysis in your deployment, Cisco recommends that you **Enable Recurring Weekly Updates from the Support Site**.

You can specify the weekly update frequency for the GeoDB. Click the time zone to change it using a pop-up window. To download the database as part of the initial configuration process, select **Install Now**.

GeoDB updates may be large and may take up to 45 minutes to install after download. You should update the GeoDB during periods of low network use.

Automatic Backups

The Firepower Management Center provides a mechanism for archiving data so configurations can be restored in case of failure. As part of the initial setup, you can **Enable Automatic Backups**.

Enabling this setting creates a scheduled task that creates a weekly backup of the configurations on the Management Center.

License Settings

You use the Firepower Management Center to manage licenses for itself and the devices it manages. The license types offered by the Firepower System depend upon the type of device you want to manage:

- For 7000 and 8000 Series, ASA FirePOWER, and NGIPSv devices, you must use Classic Licenses. Devices that use Classic Licenses are sometimes referred to as Classic devices.
- For Firepower Threat Defense physical and virtual devices, you must use Smart Licenses.

Before you add a classic license to the Firepower Management Center, make sure you have the PAK provided by Cisco when you purchased the license. If you have a legacy, pre-Cisco license, contact Support.

Note: You must enable Classic Licenses on your managed devices before you can use licensed features. You can enable a license during the initial setup of the Firepower Management Center, when you add a device to the Firepower Management Center, or by editing the device's general properties after you add the device.

Procedure

1. Obtain the License Key for your chassis during the initial setup from the License Settings section of the initial setup page.

   The License Key is clearly labeled; for example, 66:18:E7:6E:D9:93:35.

   Note: You can find the License Key on a Firepower Management Center at any time when you click the **Add New License** button from the **System>Licenses>Classic Licenses** page.

2. To obtain your license, navigate to https://www.cisco.com/go/license/ where you will be prompted for the license key (66:18:E7:6E:D9:93:35) and the Product Authorization Key (PAK).

   Note: If you ordered additional licenses, you can enter the PAKs separated commas for those licenses at the same time.

3. Follow the on-screen instructions to generate a license or licenses, which will be emailed to you.

4. Paste the license or licenses in the validation box click **Add/Verify**.

What to Do Next

- Continue with initial setup.

Note: If you have devices that use Cisco Smart Licensing, you use the **System>Licenses>Smart Licenses** page to add and verify licenses. Refer to the product documentation for those devices for information on how to add Smart Licenses to the Firepower Management Center. The *Firepower Management Center Configuration Guide* provides more information about Classic Licenses and Smart Licenses, the types of licenses for each class, and how to manage the licenses across your deployment.

Device Registration

A Firepower Management Center can manage any device, physical or virtual, currently supported by the Firepower System. You **must** configure remote management on the device before you can register the device to a Management Center.

If you are using Firepower System Version 6.0 or greater, see the device management information in the *Firepower Management Center Configuration Guide* for instructions on registering your devices.

If you are using a Firepower System Version previous to 6.0, you can add 7000 and 8000 Series devices to the Management Center during the initial setup process. However, if a device and the Management Center are separated by a NAT device, you must add it after the setup process completes; see the *Firepower 7000 and 8000 Series Installation Guide*.

You must configure both traffic channels to use the same management interface when you use a non-default management interface to connect your Management Center and managed device and those appliances are separated by a NAT device. See "Deploying on a Management Network" in the *Firepower 7000 and 8000 Series Installation Guide* for more information.

When you register a managed device to a Management Center, leave the **Apply Default Access Control Policies** check box enabled if you want to automatically apply access control policies to devices upon registration. Note that you cannot choose which policy the Management Center applies to each device, only whether to apply them. The policy that is applied to each device depends on the detection mode (see Setting Up Firepower Managed Devices in the *Firepower 7000 and 8000 Series Installation Guide*) you chose when configuring the device, as listed in the following table.

Table 1 Default Access Control Policy Applied Per Detection Mode

Detection Mode	Default Access Control Policy
Inline	Default Intrusion Prevention
Passive	Default Intrusion Prevention
Access Control	Default Access Control
Network Discovery	Default Network Discovery

An exception occurs if you previously managed a device with a Management Center and you changed the device's initial interface configuration. In this case, the policy applied by this new Management Center page depends on the changed (current) configuration of the device. If there are interfaces configured, the Management Center applies the Default Intrusion Prevention policy. Otherwise, the Management Center applies the Default Access Control policy.

If a device is incompatible with an access control policy, the policy apply fails. This incompatibility could occur for multiple reasons, including licensing mismatches, model restrictions, passive vs inline issues, and other misconfigurations. If the initial access control policy apply fails, the initial network discovery policy apply also fails. After you resolve the issue that caused the failure, you must manually apply access control and network discovery policies to the device. For more information about issues that could cause access control policy apply to fail, see the *Firepower Management Center Configuration Guide*.

To add a device, type its **Hostname** or **IP Address**, as well as the **Registration Key** you specified when you registered the device. Remember this is a simple key that you specified, up to 37 characters in length, and is not the same as a license key.

Then, use the check boxes to add licensed capabilities to the device. You can only select licenses you have already added to the Management Center; see License Settings, page 15.

Not all licenses are supported on all managed devices. However, the setup page does **not** prevent you from enabling unsupported licenses on managed devices, or enabling a capability for which you do not have a model-specific license. This is because the Management Center does not determine the device model until later. The system cannot enable an invalid license, and attempting to enable an invalid license does not decrement your available license count.

After you enable licenses, click **Add** to save the device's registration settings and, optionally, add more devices. If you selected the wrong options or mis-typed a device name, click **Delete** to remove it. You can then re-add the device.

End User License Agreement

Read the EULA carefully and, if you agree to abide by its provisions, select the check box. Make sure that all the information you provided is correct, and click **Apply**.

The Management Center is configured according to your selections. You are logged into the web interface as the `admin` user, which has the Administrator role. Continue with step 3. in Initial Setup Page: Management Centers, page 13 to complete the initial setup of the Management Center.

Administration Recommendations

After you complete the initial setup process for an appliance and verify its success, Cisco recommends that you complete various administrative tasks that make your deployment easier to manage. You should also complete any tasks you skipped during the initial setup, such as device registration and licensing. For detailed information on any the tasks described in the following sections, as well as information on how you can begin to configure your deployment, see the *Firepower Management Center Configuration Guide* for your software version.

Individual User Accounts

After you complete the initial setup, the only user on the system is the `admin` user, which has the Administrator role and access. Users with that role have full menu and configuration access to the system, including via the shell or CLI. Cisco recommends that you limit the use of the `admin` account (and the Administrator role) for security and auditing reasons.

Note: The `admin` accounts for accessing a Firepower Management Center via the shell versus accessing a Firepower Management Center via the web interface are not the same, and may use different passwords.

Creating a separate account for each person who will use the system allows your organization not only to audit actions and changes made by each user, but also to limit each person's associated user access role or roles. This is especially important on the Management Center, where you perform most of your configuration and analysis tasks. For example, an analyst needs access to event data to analyze the security of your network, but may not require access to administrative functions for the deployment.

The system includes ten predefined user roles designed for a variety of administrators and analysts. You can also create custom user roles with specialized access privileges.

Device Registration

For all Firepower versions you can register devices to the FMC after completing the FMC initial setup.

Note: If you are using a Firepower System version previous to 6.0, you can add 7000 and 8000 Series devices to the Management Center during the initial setup process; see Device Registration, page 16 for information.

A Firepower Management Center can manage any device, physical or virtual, currently supported by your version of the Firepower System. Depending on your Firepower version this may include:

- Firepower 7000 and 8000 Series appliances—physical devices purpose-built for theFirepower System. Firepower 7000 and 8000 Series devices have a range of throughputs, but share most of the same capabilities. In general, 8000 Series devices are more powerful than 7000 Series devices; they also support additional features such as 8000 Series fastpath rules, link aggregation, and stacking. You must configure remote management on the device before you can register the device to a Firepower Management Center.
- NGIPSv—a 64-bit virtual device deployed in the VMware VSphere environment. NGIPSv devices do not support any of the system's hardware-based features such as redundancy and resource sharing, switching, and routing.
- Cisco ASA with FirePOWER Services (or an *ASA FirePOWER module*)—provides the first-line system policy and passes traffic to the Firepower System for discovery and access control. However, you cannot use the Firepower Management Center web interface to configure ASA FirePOWER interfaces. Cisco ASA with FirePOWER Services has a software and command line interface (CLI) unique to the ASA platform to install the system and to perform other platform-specific administrative tasks.
- Firepower Threat Defense—provides a unified next-generation firewall and next-generation IPS device.
- Firepower Threat Defense Virtual—a 64-bit virtual device that is designed to work in multiple hypervisor environments, reduce administrative overhead, and increase operational efficiency.

To register managed devices to a Firepower Management Center, see the device management information in the *Firepower Management Center Configuration Guide* for your software version. For information on compatibility among Firepower devices and software versions, see the *Cisco Firepower Compatibility Guide*.

Health and System Policies

By default, all appliances have an initial system policy applied. The system policy governs settings that are likely to be similar for multiple appliances in a deployment, such as mail relay host preferences and time synchronization settings. Cisco recommends that you use the Management Center to apply the same system policy to itself and all the devices it manages.

By default, the Management Center also has a health policy applied. A health policy, as part of the health monitoring feature, provides the criteria for the system continuously monitoring the performance of the appliances in your deployment. Cisco recommends that you use the Management Center to apply a health policy to all the devices it manages.

Software and Database Updates

You should update the system software on your appliances before you begin any deployment. Cisco recommends that all the appliances in your deployment run the most recent version of the Firepower System. If you are using them in your deployment, you should also install the latest intrusion rule updates, VDB, and GeoDB. For Versions 6.5+, the Initial Configuration Wizard automatically configures some of these update activities for you; see Automatic Initial Configuration, page 9 for more information.

Caution: Before you update any part of the Firepower System, you must read the release notes or advisory text that accompanies the update. The release notes provide important information, including supported platforms, compatibility, prerequisites, warnings, and specific installation and uninstallation instructions.

Redirecting Console Output

By default, Management Centers direct initialization status, or *init*, messages to the VGA port. If you want to use the physical serial port or SOL to access the console, Cisco recommends you redirect console output to the serial port after you complete the initial setup.

To redirect console output using the shell, you run a script from the appliance's shell.

Using the Shell to Redirect the Console Output

Procedure

1. Using your keyboard/monitor or serial connection, log into the appliance's shell using an account with Administrator privileges. Use the steps appropriate to your Firepower version; see Accessing the CLI or the Linux Shell on the FMC, page 3.

   The prompt for the appliance appears.
2. At the prompt, set the console output by typing one of the following commands:
   - To access the appliance using the VGA port:

     ```
     sudo /usr/local/sf/bin/configure_console.sh vga
     ```
   - To access the appliance using the physical serial port:

     ```
     sudo /usr/local/sf/bin/configure_console.sh serial
     ```
   - To access the appliance using LOM via SOL:

     ```
     sudo /usr/local/sf/bin/configure_console.sh sol
     ```
3. To implement your changes, reboot the appliance by typing `sudo reboot`.

   The appliance reboots.

Using the Web Interface to Redirect the Console Output

Procedure

1. Select **System > Configuration**.

2. Select **Console Configuration**.
3. Select a remote console access option:
   - Select **VGA** to use the appliance's VGA port. This is the default option.
   - Select **Physical Serial Port** to use the appliance's serial port, or to use LOM/SOL on a Management Center.

   If you selected **Physical Serial Port**, the LOM settings appear.
4. To configure LOM via SOL, enter the appropriate settings:
   - **DHCP Configuration** for the appliance (**DHCP** or **Static**).
   - **IP Address** to be used for LOM. The LOM IP address must be different from the management interface IP address of the appliance.
   - **Netmask** for the appliance.
   - **Default Gateway** for the appliance.
5. Click **Save**.

Remote console configuration for the appliance is saved. If you configured Lights-Out Management, you must enable it for at least one user; see Enabling LOM and LOM Users, page 37.

Setting Up Lights-Out Management

If you need to restore a Firepower device to factory defaults and do not have physical access to the appliance, you can use Lights-Out Management (LOM) to perform the restore process. Note that you can use Lights-Out Management on the default (`eth0`) management interface only.

The LOM feature allows you to perform a limited set of actions on a Firepower device, using a Serial over LAN (SOL) connection. With LOM, you use a command line interface on an out-of-band management connection to perform tasks such as viewing the chassis serial number, or monitoring conditions such as fan speed and temperature.

Caution: The Firepower Management Center 2000 and 4000 introduced Cisco's Unified Computing System (UCS) platform into the Firepower System. These models do not support Cisco functionality that uses tools on the baseboard management controller (BMC), such as the UCS Manager or the Cisco Integrated Management Controller (CIMC), to make any configuration changes or firmware updates.

The syntax of LOM commands depends on the utility you are using, but LOM commands generally contain the elements listed in the following table.

Table 2 LOM Command Syntax

IPMItool (Linux/Mac)	ipmiutil (Windows)	Description
ipmitool	ipmiutil	Invokes the IPMI utility.
n/a	-V4	For ipmiutil only, enables admin privileges for the LOM session.
-I lanplus	-J3	Enables encryption for the LOM session.
-H *IP_address*	-N *IP_address*	Specifies the IP address of the management interface on the appliance.

Table 2 LOM Command Syntax (continued)

IPMItool (Linux/Mac)	ipmiutil (Windows)	Description
-U *username*	-U *username*	Specifies the user name of an authorized LOM account.
n/a (prompted on login)	-P *password*	For ipmiutil only, specifies the password for an authorized LOM account.
command	command	The command you want to issue to the appliance. Note that where you issue the command depends on the utility: ■ For IPMItool, type the command last. ■ For ipmiutil, type the command first.

Therefore, for IPMItool:

```
ipmitool -I lanplus -H IP_address -U username command
```

Or, for ipmiutil:

```
ipmiutil command -V4 -J3 -N IP_address -U username -P password
```

Note that the `chassis power off` and `chassis power cycle` commands are not valid on 70xx Family appliances. For a full list of LOM commands supported by the Firepower System, see the Configuring Appliance Settings chapter in the *Firepower Management Center Configuration Guide*.

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.

Before you can restore an appliance using LOM, you must enable LOM for both the appliance and the user who will perform the restore. Then, use a third-party Intelligent Platform Management Interface (IPMI) utility to access the appliance. You must also make sure you redirect the appliance's console output to the serial port.

For more information, see the following sections:

- Enabling LOM and LOM Users, page 37
- Installing an IPMI Utility, page 38

Enabling LOM and LOM Users

Before you can use LOM to restore an appliance, you must enable and configure the feature. You must also explicitly grant LOM permissions to users who will use the feature.

You configure LOM and LOM users on a per-appliance basis using each appliance's local web interface. That is, you cannot use the Management Center to configure LOM on a Firepower device. Similarly, because users are managed independently per appliance, enabling or creating a LOM-enabled user on the Management Center does not transfer that capability to users on Firepower devices.

LOM users also have the following restrictions:

- You must assign the Administrator role to the user.
- The user name may have up to 16 alphanumeric characters. Hyphens and longer user names are not supported for LOM users.

- The password may have up to 20 alphanumeric characters. Longer passwords are not supported for LOM users. A user's LOM password is the same as that user's system password.
- Management Centers can have up to 13 LOM users.

Note: For detailed instructions on the following tasks, see the Configuring Appliance Settings chapter in the *Firepower Management Center Configuration Guide*.

To enable LOM:

1. Select **System > Configuration**, then click **Console Configuration**.
2. For **Console**, choose **Physical Serial Port**.
3. Specify the LOM IP address, netmask, and default gateway (or use DHCP to have these values automatically assigned).

Note: The LOM IP address must be different from the management interface IP address of the appliance.

To enable LOM capabilities for a Firepower System user:

1. Select **System > User Management**, then either edit an existing user to add LOM permissions, or create a new user that you will use for LOM access to the appliance.
2. On the User Configuration page, enable the **Administrator** role if it is not already enabled.
3. Enable the **Allow Lights-Out Management Access** check box and save your changes.

Installing an IPMI Utility

You use a third-party IPMI utility on your computer to create an SOL connection to the appliance.

If your computer is running Linux or Mac OS, use IPMItool. Although IPMItool is standard with many Linux distributions, you must install IPMItool on a Mac. First, confirm that your Mac has Apple's xCode developer tools package installed. Also, make sure the optional components for command line development are installed ("UNIX Development" and "System Tools" in newer versions, or "Command Line Support" in older versions). Finally, install MacPorts and IPMItool. For more information, use your favorite search engine or see these sites:

```
https://developer.apple.com/technologies/tools/
http://www.macports.org/
```

For Windows environments, use ipmiutil, which you must compile yourself. If you do not have access to a compiler, you can use ipmiutil itself to compile. For more information, use your favorite search engine or see this site:

```
http://ipmiutil.sourceforge.net/
```

Restoring a Firepower Management Center to Factory Defaults

Cisco provides ISO images on its Support Site for restoring, or reimaging, Firepower Management Centers to their original factory settings.

For more information, see the following sections:

- Before You Begin, page 23
- Understanding the Restore Process, page 24
- Obtaining the Restore ISO and Update Files, page 25
- Beginning the Restore Process, page 25

Before You Begin

Before you begin restoring your appliances to factory defaults, you should familiarize yourself with the expected behavior of the system during the restore process.

Reimaging Version 5.x Hardware to Version 6.3+

Because of a change to ISO image names, you cannot freshly install Version 6.3+ on a physical Firepower appliance that is currently running Version 5.x. This includes the following Firepower Management Centers models covered in this guide:

- 750, 1500, 1500
- 2000, 4000

The quickest path to Version 6.3 is:

1. Freshly install Version 6.2.3, then
2. Freshly install (or upgrade to) Version 6.3+.

Note: After you reimage a Version 5.x Defense Center/Management Center to a Version 6.2.3 Firepower Management Center, it cannot manage its older devices. You should also reimage those devices, then re-add them to the Management Center.

See the Firepower Release Notes for more information about the change to ISO image name.

Configuration and Event Backup Guidelines

Before you begin the restore process, Cisco recommends that you delete or move any backup files that reside on your appliance, then back up current event and configuration data to an external location.

Restoring your appliance to factory defaults results in the loss of almost **all** configuration and event data on the appliance. Although the restore utility can retain the appliance's license, network, and (in some cases) Lights-Out Management (LOM) settings, you must perform all other setup tasks after the restore process completes.

Retention of LOM settings after the restore process varies by model and Firepower version:

- If you are restoring an FMC model 750, 1500, or 3500 to factory defaults, deleting the license and network settings also resets the LOM settings.

Caution: When restoring FMC models 750, 1500, or 3500 to factory settings using LOM, if you do not have physical access to the appliance and you delete the license and network settings, you will be unable to access the FMC after the restore.

- If you are restoring an FMC model 2000 or 4000 to factory defaults:
  - If you restore the FMC to Version 6.2.3 or earlier, the system does *not* reset LOM settings regardless of whether you choose to delete the license and network settings.
  - If you restore the FMC to Version 6.3+, the system resets LOM settings regardless of whether you choose to delete the license and network settings.

Caution: When restoring FMC models 2000 or 4000 to Version 6.3+ using LOM, if you do not have physical access to the appliance and you delete the license and network settings, you will be unable to access the FMC after the restore.

Traffic Flow During the Restore Process

To avoid disruptions in traffic flow on your network, Cisco recommends restoring your appliances during a maintenance window or at a time when the interruption will have the least impact on your deployment.

Restoring a Firepower device that is deployed inline resets the device to a non-bypass (fail closed) configuration, disrupting traffic on your network. Traffic is blocked until you configure bypass-enabled inline sets on the device. For more information about editing your device configuration to configure bypass, see the Managing Devices chapter of the *Firepower Management Center Configuration Guide*.

Understanding the Restore Process

To restore a Firepower device, you boot from the appliance's internal flash drive and use an interactive menu to download and install the ISO image on the appliance. For your convenience, you can install system software and intrusion rule updates as part of the restore process.

Only reimage your appliances during a maintenance window. Reimaging resets appliances in bypass mode to a non-bypass configuration and disrupts traffic on your network until you reconfigure bypass mode. For more information, see Traffic Flow During the Restore Process, page 24.

Note that you **cannot** restore an appliance using its web interface. To restore an appliance, you must connect to it in one of the following ways:

Keyboard and Monitor/KVM

You can connect a USB keyboard and VGA monitor to the appliance, which is useful for rack-mounted appliances connected to a KVM (keyboard, video, and mouse) switch. If you have a KVM that is remote-accessible, you can restore appliances without having physical access.

Serial Connection/Laptop

You can use a rollover serial cable (also known as a NULL modem cable or a Cisco console cable) to connect a computer to the appliance. See the hardware specifications for your appliance to locate the serial port. To interact with the appliance, use terminal emulation software such as HyperTerminal or XModem.

Lights-Out Management Using Serial over LAN

You can perform a limited set of actions on Management Centers and Firepower devices using Lights-Out Management (LOM) with a Serial over LAN (SOL) connection. If you do not have physical access to an appliance, you can use LOM to perform the restore process. After you connect to an appliance using LOM, you issue commands to the restore utility as if you were using a physical serial connection. Note that you can use Lights-Out Management on the default (`eth0`) management interface only. For more information, see Setting Up Lights-Out Management, page 36.

Before You Begin

- Obtain the restore ISO image for the appliance from the Support Site. See Obtaining the Restore ISO and Update Files, page 25.
- Reimaging a Firepower Management Center could cause an Out of Compliance (OOC) state with the Cisco License Authority. As a best practice, when reimaging a Firepower Management Center, first deregister the Firepower Management Center from the Cisco Smart Software Manager. Choose **System > Licenses > Smart Licenses** and click the deregister icon.

To restore a Firepower device:

1. Copy the image to an appropriate storage medium.
2. Connect to the appliance.

3. Reboot the appliance and invoke the restore utility.

What to Do Next

- Install the ISO image using the procedure in Beginning the Restore Process, page 25.

Obtaining the Restore ISO and Update Files

Cisco provides ISO images for restoring appliances to their original factory settings. Before you restore an appliance, obtain the correct ISO image from the Support Site.

The ISO image you should use to restore an appliance depends on when Cisco introduced support for that appliance model. Unless the ISO image was released with a minor version to accommodate a new appliance model, ISO images are usually associated with major versions of the system software (for example, 5.2 or 5.3). To avoid installing an incompatible version of the system, Cisco recommends that you always use the most recent ISO image available for your appliance.

Firepower devices use an internal flash drive to boot the appliance so you can run the restore utility.

Cisco also recommends that you always run the latest version of the system software supported by your appliance. After you restore an appliance to the latest supported major version, you should update its system software, intrusion rules, and Vulnerability Database (VDB). For more information, see the release notes for the update you want to apply, as well as the *Firepower Management Center Configuration Guide*.

For your convenience, you can install system software and intrusion rule updates as part of the restore process. For example, you could restore a device to Version 6.0, and also update the device to Version 6.0.0.1 as part of that process. Keep in mind that only Management Centers require rule updates.

To obtain the restore ISO and other update files:

1. Using the user name and password for your support account, log into the Support Site (https://sso.cisco.com/autho/forms/CDClogin.html).
2. Browse to the software download section (https://software.cisco.com/download/navigator.html).
3. Enter a search string in the **Find** area on the page that appears for the system software you want to download and install.

   For example, to find software downloads for Firepower, you would enter **Firepower**.
4. Find the image (ISO image) that you want to download.

   You can click one of the links on the left side of the page to view the appropriate section of the page. For example, you would click **6.0 Images** to view the images and release notes for Version 6.0 of the Firepower System.
5. Click the ISO image you want to download.

   The file begins downloading.
6. Copy the files to an HTTP (web) server, FTP server, or SCP-enabled host that the appliance can access on its management network.

Caution: Do not transfer ISO or update files via email; the files can become corrupted. Also, do not change the names of the files; the restore utility requires that they be named as they are on the Support Site.

Beginning the Restore Process

Begin the restore process by booting the appliance from an internal flash drive.

After you make sure that you have the appropriate level of access and connection to an appliance, as well the correct ISO image, use one of the following procedures to restore your appliance:

- Starting the Restore Utility Using KVM or Physical Serial Port, page 26 explains how to start the restore process for an appliance where you do not have LOM access.
- Starting the Restore Utility Using Lights-Out Management, page 27 explains how use LOM to start the restore process via an SOL connection.

Caution: The procedures in this chapter explain how to restore an appliance without powering it down. However, if you need to power down for any reason, use the appliance's web interface, the `system shutdown` command from the CLI, or the `shutdown -h now` command from an appliance's shell (sometimes called expert mode).

Starting the Restore Utility Using KVM or Physical Serial Port

For Firepower devices, Cisco provides a restore utility on an internal flash drive.

Note: Do **not** use a KVM console with USB mass storage to access the appliance for the initial setup because the appliance may attempt to use the mass storage device as a boot device.

If you need to restore an appliance to factory defaults and do not have physical access, you can use LOM to perform the restore process; see Starting the Restore Utility Using Lights-Out Management, page 27.

To start the restore utility:

1. Using your keyboard/monitor or serial connection, log into the appliance using the `admin` account. Use the steps appropriate to your Firepower version; see Accessing the CLI or the Linux Shell on the FMC, page 3.
2. Reboot the appliance; type `sudo reboot`. Provide the `admin` password when prompted.
3. Monitor the reboot status:
   - If the system is performing a database check, you may see the following message:

     ```
     The system is not operational yet. Checking and repairing database are in progress.
     This may take a long time to finish.
     ```

   - For a keyboard and monitor connection, quickly press one of the arrow keys repeatedly to prevent the appliance from booting the currently installed version of the system.
   - For a serial connection, when you see the BIOS boot options, press Tab slowly and repeatedly to prevent the appliance from booting the currently installed version of the system.
4. The system responds differently depending on the hardware model and type of connection:

   For models 750, 1500, or 3500:

   - **For a keyboard and monitor connection:**

     The red LILO menu appears offering three options: to boot the current version of the system, perform a system restore using the standard console (**System_Restore**), or perform a system restore using a serial connection (**Restore_Serial**). Use the arrow keys to select **System_Restore** and press Enter.

   - **For a serial connection:**

     The LILO boot prompt appears. For example:

     ```
     LILO 24.2 boot:
     6.4.0          System_Restore       Restore_Serial
     boot:
     ```

     Type `Restore_Serial` and press Enter.

   For models 2000 and 4000:

   - **For a keyboard and monitor connection:**

The red LILO menu appears offering two options: to restore the current version of the system, or to perform a system restore (**System_Restore**). Use the arrow keys to select **System_Restore** and press Enter.

The `boot`: prompt appears after the following choices:

```
0. Load with standard console
1. Load with serial console
```

Type `0` and press Enter.

– **For a serial connection:**

The LILO boot prompt appears. For example:

```
LILO 24.2 boot:
6.4.0          System_Restore
boot:
```

Type `System_Restore` and press Enter.

The `boot`: prompt appears after the following choices:

```
0. Load with standard console
1. Load with serial console
```

Type `1` and press Enter.

5. Press Enter to confirm the copyright notice.
6. Unless this is the first time you have restored the appliance to this major version, the utility automatically loads the last restore configuration you used. To continue, confirm the settings in a series of pages until the "Cisco Firepower Appliance <Version> Configuration Menu" appears.

What to Do Next

- Continue with Using the Interactive Menu to Restore an Appliance, page 28.

Starting the Restore Utility Using Lights-Out Management

If you need to restore an appliance to factory defaults and do not have physical access to the appliance, you can use LOM to perform the restore process. Note that you can use Lights-Out Management on the default (`eth0`) management interface only.

Caution: When restoring FMC models 750, 1500, or 3500 to factory settings using LOM, if you do not have physical access to the appliance and you delete the license and network settings, you will be unable to access the FMC after the restore.

Caution: When restoring FMC models 2000 or 4000 to Version 6.3+ using LOM, if you do not have physical access to the appliance and you delete the license and network settings, you will be unable to access the FMC after the restore.

Note: Before you can restore an appliance using LOM, you must enable the feature; see Setting Up Lights-Out Management, page 36.

To start the restore utility using Lights-Out Management:

1. Access the Linux shell using the `admin` account. Use the steps appropriate to your Firepower version; see Accessing the CLI or the Linux Shell on the FMC, page 3.
2. At your computer's command prompt, enter the IPMI command to start the SOL session:

   For IPMItool, type:

```
sudo ipmitool -I lanplus -H IP_address -U username sol activate
```

For ipmiutil, type:

```
sudo ipmiutil sol -a -V4 -J3 -N IP_address -U username -P password
```

Where *IP_address* is the IP address of the management interface on the appliance, *username* is user name of an authorized LOM account, and *password* is the password for that account. Note that IPMItool prompts you for the password after you issue the **sol activate** command.

3. Reboot the appliance; type `sudo reboot`. Provide the `admin` password when prompted.
4. Monitor the reboot status.

   If the system is performing a database check, you may see the following message:

   ```
   The system is not operational yet. Checking and repairing database are in progress.
   This may take a long time to finish.
   ```

   When you see the BIOS boot options, press Tab slowly and repeatedly (to prevent the appliance from booting the currently installed version of the system) until the LILO boot prompt appears. For example:

   ```
   GNU/Linux - LILO 24 - Boot Menu
   6.1.0
   System_Restore
   Restore_Serial
   ```

5. At the boot prompt, start the restore utility by typing **Restore_Serial**.

   The boot prompt appears after the following choices:

   ```
   0. Load with standard console
   1. Load with serial console
   ```

6. Type `1` and press Enter to load the interactive restore menu via the appliance's serial connection.

Note: If you do not select a display mode, the restore utility defaults to the standard console after 30 seconds.

7. Press Enter to confirm the copyright notice.
8. Unless this is the first time you have restored the appliance to this major version, the utility automatically loads the last restore configuration you used. To continue, confirm the settings in a series of pages until the "Cisco Firepower Appliance <Version> Configuration Menu" appears.

What to Do Next

- Continue with Using the Interactive Menu to Restore an Appliance, page 28.

Using the Interactive Menu to Restore an Appliance

The restore utility for Firepower devices uses an interactive menu to guide you through the restoration.

Note: Only reimage your appliances during a maintenance window. Reimaging resets appliances in bypass mode to a non-bypass configuration and disrupts traffic on your network until you reconfigure bypass mode. For more information, see Traffic Flow During the Restore Process, page 24.

The menu displays the options listed in the following table.

Table 3 Restore Menu Options

Option	Description	For more information, see...
1 IP Configuration	Specify network information about the management interface on the appliance you want to restore, so that the appliance can communicate with the server where you placed the ISO and any update files.	Identifying the Appliance's Management Interface, page 30
2 Choose the transport protocol	Specify the location of the ISO image you will use to restore the appliance, as well as any credentials the appliance needs to download the file.	Specifying ISO Image Location and Transport Method, page 30
3 Select Patches/Rule Updates	Specify a system software and intrusion rules update to be applied after the appliance is restored to the base version in the ISO image.	Updating System Software and Intrusion Rules During Restore, page 31
4 Download and Mount ISO	Download the appropriate ISO image and any system software or intrusion rule updates. Mount the ISO image.	Downloading the ISO and Update Files and Mounting the Image, page 32
5 Run the Install	Invoke the restore process.	Invoking the Restore Process, page 32
6 Save Configuration 7 Load Configuration	Save any set of restore configurations for later use, or load a saved set.	Saving and Loading Restore Configurations, page 34
8 Wipe Contents of Disk	Securely scrub the hard drive to ensure that its contents can no longer be accessed.	Scrubbing the Hard Drive, page 41

Navigate the menu using your arrow keys. To select a menu option, use the up and down arrows. Use the right and left arrow keys to toggle between the **OK** and **Cancel** buttons at the bottom of the page.

The menu presents two different kinds of options:

- To select a numbered option, first highlight the correct option using the up and down arrows, then press Enter while the **OK** button at the bottom of the page is highlighted.
- To select a multiple-choice (radio button) option, first highlight the correct option using the up and down keys, then press the space bar to mark that option with an x. To accept your selection, press Enter while the **OK** button is highlighted.

In most cases, complete menu options **1**, **2**, **4**, and **5**, in order. Optionally, add menu option **3** to install system software and intrusion rule updates during the restore process.

If you are restoring an appliance to a different major version from the version currently installed on the appliance, a two-pass restore process is required. The first pass updates the operating system, and the second pass installs the new version of the system software.

If this is your second pass, or if the restore utility automatically loaded the restore configuration you want to use, you can start with menu option **4**: Downloading the ISO and Update Files and Mounting the Image, page 32. However, Cisco recommends you double-check the settings in the restore configuration before proceeding.

Note: To use a previously saved configuration, start with menu option **6**: Saving and Loading Restore Configurations, page 34. After you load the configuration, skip to menu option **4**: Downloading the ISO and Update Files and Mounting the Image, page 32.

To restore an appliance using the interactive menu, use the following steps:

1. **1 IP Configuration** — see Identifying the Appliance's Management Interface, page 30.
2. **2 Choose the transport protocol** — see Specifying ISO Image Location and Transport Method, page 30.

3. **3 Select Patches/Rule Updates** (optional) — Updating System Software and Intrusion Rules During Restore, page 31.
4. **4 Download and Mount ISO** — see Downloading the ISO and Update Files and Mounting the Image, page 32.
5. **5 Run the Install** — see Invoking the Restore Process, page 32.

Identifying the Appliance's Management Interface

The first step in running the restore utility is to identify the management interface on the appliance you want to restore, so that the appliance can communicate with the server where you copied the ISO and any update files. If you are using LOM, remember that the management IP address for the appliance is **not** the LOM IP address.

To identify the appliance's management interface:

1. From the restore utility main menu, select **1 IP Configuration**.
2. Select the appliance's management interface (generally **eth0**).
3. Select the protocol you are using for your management network: **IPv4** or **IPv6**.

   Options for assigning an IP address to the management interface appear.
4. Select a method to assign an IP address to the management interface: **Static** or **DHCP**:
   - If you select **Static**, a series of pages prompts you to manually enter the IP address, network mask or prefix length, and default gateway for the management interface.
   - If you select **DHCP**, the appliance automatically detects the IP address, network mask or prefix length, and default gateway for the management interface, then displays the IP address.
5. When prompted, confirm your settings.

   If prompted, confirm the IP address assigned to the appliance's management interface.

What to Do Next

- Continue with the next section, Specifying ISO Image Location and Transport Method.

Specifying ISO Image Location and Transport Method

After you configure the management IP address that the restore process will use to download files it needs, you must identify which ISO image you will use to restore the appliance. This is the ISO image that you downloaded from the Support Site (see Obtaining the Restore ISO and Update Files, page 25), and stored on a web server, FTP server, or SCP-enabled host.

The interactive menu prompts you to enter any necessary information to complete the download, as listed in the following table.

Table 4 Information Needed to Download Restore Files

To use...	You must provide...
HTTP	■ IP address for the web server ■ full path to the ISO image directory (for example, `/downloads/ISOs/`)
FTP	■ IP address for the FTP server ■ path to the ISO image directory, relative to the home directory of the user whose credentials you want to use (for example, `mydownloads/ISOs/`) ■ authorized user name and password for the FTP server
SCP	■ IP address for the SCP server ■ authorized user name for the SCP server ■ full path to the ISO image directory ■ password for the user name you entered earlier Note that before you enter your password, the appliance may ask you to add the SCP server to its list of trusted hosts. You must accept to continue.

Note that the restore utility will also look for update files in the ISO image directory.

To specify the restore files' location and transport method:

1. From the restore utility main menu, select **2 Choose the transport protocol**.
2. On the page that appears, select either **HTTP**, **FTP**, or **SCP**.
3. Use the series of pages presented by the restore utility to provide the necessary information for the protocol you chose, as described in Table 4 on page -31.

   If your information was correct, the appliance connects to the server and displays a list of the Cisco ISO images in the location you specified.
4. Select the ISO image you want to use.
5. When prompted, confirm your settings.
6. Do you want to install a system software or intrusion rule update as a part of the restore process?
   - If yes, continue with the next section, Updating System Software and Intrusion Rules During Restore.
   - If no, continue with Downloading the ISO and Update Files and Mounting the Image, page 32. Note that you can use the system's web interface to manually install updates after the restore process completes.

Updating System Software and Intrusion Rules During Restore

Optionally, you can use the restore utility to update the system software and intrusion rules after the appliance is restored to the base version in the ISO image. Note that only Management Centers require rule updates.

The restore utility can only use one system software update and one rule update. However, system updates are cumulative back to the last major version; rule updates are also cumulative. Cisco recommends that you obtain the latest updates available for your appliance; see Obtaining the Restore ISO and Update Files, page 25.

If you choose not to update the appliance during the restore process, you can update later using the system's web interface. For more information, see the release notes for the update you want to install, as well as the Updating System Software chapter in the *Firepower Management Center Configuration Guide*.

To install updates as part of the restore process:

1. From the restore utility main menu, select **3 Select Patches/Rule Updates**.

   The restore utility uses the protocol and location you specified in the previous procedure (see Specifying ISO Image Location and Transport Method, page 30) to retrieve and display a list of any system software update files in that location. If you are using SCP, enter your password when prompted to display the list of update files.

2. Select the system software update, if any, you want to use.

   You do not have to select an update; press Enter without selecting an update to continue. If there are no system software updates in the appropriate location, the system prompts you to press Enter to continue.

   The restore utility retrieves and displays a list of rule update files. If you are using SCP, enter your password when prompted to display the list.

3. Select the rule update, if any, you want to use.

   You do not have to select an update; press Enter without selecting an update to continue. If there are no rule updates in the appropriate location, the system prompts you to press Enter to continue.

What to Do Next

- Continue with the next section, Downloading the ISO and Update Files and Mounting the Image.

Downloading the ISO and Update Files and Mounting the Image

The final step before you invoke the restore process is to download the necessary files and mount the ISO image.

Before You Begin

- Before you begin this step, you may want to save your restore configuration for later use. For more information, see Saving and Loading Restore Configurations, page 34.

To download and mount the ISO image:

1. From the restore utility main menu, select **4 Download and Mount ISO**.
2. When prompted, confirm your choice. If you are downloading from an SCP server, enter your password when prompted.

   The appropriate files are downloaded and mounted.

What to Do Next

- Continue with the next section, Invoking the Restore Process.

Invoking the Restore Process

After you download and mount the ISO image, you are ready to invoke the restore process. If you are restoring an appliance to a different major version from the version currently installed on the appliance, a two-pass restore process is required. The first pass updates the operating system, and the second pass installs the new version of the system software.

First Pass of Two (Changing Major Versions Only)

When restoring an appliance to a different major version, a first pass by the restore utility updates the appliance's operating system, and, if necessary, the restore utility itself.

Note: If you are restoring an appliance to the same major version, or if this is your second pass through the process, skip to the next procedure: Second or Only Pass, page 33.

To perform the first pass of a two-pass restore process:

1. From the restore utility main menu, select **5 Run the Install**.
2. When prompted (twice), confirm that you want to reboot the appliance.
3. Monitor the reboot and invoke the restore process again:

   If the system is performing a database check, you may see the following message:

   ```
   The system is not operational yet. Checking and repairing database are in progress.
   This may take a long time to finish.
   ```

   For a keyboard and monitor connection, quickly press one of the arrow keys to prevent the appliance from booting the currently installed version of the system.

   For a serial or SOL/LOM connection, when you see the BIOS boot options, press Tab slowly and repeatedly until the LILO boot prompt appears. For example:

   ```
   GNU/Linux - LILO 24 - Boot Menu
   6.1.0
   System_Restore
   Restore_Serial
   ```

4. Indicate that you want to restore the system:
   - For a keyboard and monitor connection, use the arrow keys to select **System_Restore** and press Enter.
   - For a serial or SOL/LOM connection, type **Restore_Serial** at the prompt and press Enter.

   In either case, the boot prompt appears after the following choices:

   ```
   0. Load with standard console
   1. Load with serial console
   ```

5. Select a display mode for the restore utility's interactive menu:
   - For a keyboard and monitor connection, type `0` and press Enter.
   - For a serial or SOL/LOM connection, type `1` and press Enter.

   If you do not select a display mode, the restore utility defaults to the standard console after 30 seconds.

   Unless this is the first time you have restored the appliance to this major version, the utility automatically loads the last restore configuration you used. To continue, confirm the settings in a series of pages.
6. Press Enter to confirm the copyright notice.

What to do Next

- Begin the second pass of the process, starting with Using the Interactive Menu to Restore an Appliance, page 28.

Second or Only Pass

Use the following procedure to perform the second or only pass through the restore process.

To perform the second or only pass through the restore process:

1. If you are performing the second pass of a two-pass restore process, download and mount the ISO image again, as described in Downloading the ISO and Update Files and Mounting the Image, page 32.
2. From the restore utility main menu, select **5 Run the Install**.

3. Confirm that you want to restore the appliance and continue with the next step.
4. Choose whether you want to delete the appliance's license and network settings.

   In most cases, you do not want to delete these settings, because it can make the initial setup process shorter. Changing settings after the restore and subsequent initial setup is often less time consuming than trying to reset them now. For more information, see Next Steps, page 35.

Caution: When restoring FMC models 750, 1500, or 3500 to factory settings using LOM, if you do not have physical access to the appliance and you delete the license and network settings, you will be unable to access the FMC after the restore.

Caution: When restoring FMC models 2000 or 4000 to Version 6.3+ using LOM, if you do not have physical access to the appliance and you delete the license and network settings, you will be unable to access the FMC after the restore.

5. Type your final confirmation that you want to restore the appliance.

   The final stage of the restore process begins. When it completes, if prompted, confirm that you want to reboot the appliance.

Caution: Make sure you allow sufficient time for the restore process to complete. On appliances with internal flash drives, the utility first updates the flash drive, which is then used to perform other restore tasks. If you quit (by pressing Ctrl + C, for example) during the flash update, you could cause an unrecoverable error. If you think the restore is taking too long or you experience any other issues with the process, do not quit. Instead, contact Support.

Note: Reimaging resets appliances in bypass mode to a non-bypass configuration and disrupts traffic on your network until you reconfigure bypass mode. For more information, see Traffic Flow During the Restore Process, page 24.

What to Do Next

- Continue with Next Steps, page 35.

Saving and Loading Restore Configurations

You can use the restore utility to save a restore configuration to use if you need to restore a Firepower device again. Although the restore utility automatically saves the last configuration used, you can save multiple configurations, which include:

- network information about the management interface on the appliance; see Identifying the Appliance's Management Interface, page 30
- the location of the restore ISO image, as well as the transport protocol and any credentials the appliance needs to download the file; see Specifying ISO Image Location and Transport Method, page 30
- the system software and intrusion rules updates, if any, that you want to apply after the appliance is restored to the base version in the ISO image; see Updating System Software and Intrusion Rules During Restore, page 31

SCP passwords are not saved. If the configuration specifies that the utility must use SCP to transfer ISO and other files to the appliance, you will have to re-authenticate to the server to complete the restore process.

The best time to save a restore configuration is after you provide the information listed above, but before you download and mount the ISO image.

To save a restore configuration:

1. From the restore utility main menu, select **6 Save Configuration**.

   The utility displays the settings in the configuration you are saving.

2. When prompted, confirm that you want to save the configuration.
3. When prompted, enter a name for the configuration.

What to Do Next

- To use the configuration you just saved to restore the appliance, continue with Downloading the ISO and Update Files and Mounting the Image, page 32.

To load a saved restore configuration:

1. From the restore utility main menu, select **7 Load Configuration**.

   The utility presents a list of saved restore configurations. The first option, **default_config**, is the configuration you last used to restore the appliance. The other options are restore configurations that you have saved.
2. Select the configuration you want to use.

   The utility displays the settings in the configuration you are loading.
3. When prompted, confirm that you want to load the configuration.

   The configuration is loaded. If prompted, confirm the IP address assigned to the appliance's management interface.

What to Do Next

- To use the configuration you just loaded to restore the appliance, continue with Downloading the ISO and Update Files and Mounting the Image, page 32.

Next Steps

Restoring your appliance to factory default settings results in the loss of almost **all** configuration and event data on the appliance. Note that deleting license and network settings also resets LOM settings in some cases.

Retention of LOM settings after the restore process varies by model and Firepower version:

- If you are restoring an FMC model 750, 1500, or 3500 to factory defaults, deleting the license and network settings also resets the LOM settings.

Caution: When restoring FMC models 750, 1500, or 3500 to factory settings using LOM, if you do not have physical access to the appliance and you delete the license and network settings, you will be unable to access the FMC after the restore.

- If you are restoring an FMC model 2000 or 4000 to factory defaults:
  - If you restore the appliance to Version 6.2.3 or earlier, the system does *not* reset LOM settings regardless of whether you choose to delete the license and network settings.
  - If you restore the appliance to Version 6.3+, the system resets LOM settings regardless of whether you choose to delete the license and network settings.

Caution: When restoring FMC models 2000 or 4000 to Version 6.3+ using LOM, if you do not have physical access to the appliance and you delete the license and network settings, you will be unable to access the FMC after the restore.

After you restore an appliance, you must complete an initial setup process:

- If you did not delete the appliance's license and network settings, you can use a computer on your management network to browse directly to the appliance's web interface to perform the setup. For more information:
  - For Versions 5.4.x – 6.4.x, see Initial Setup Page: Management Centers, page 13.

  - For Versions 6.5+, see Firepower Management Center Initial Configuration Wizard, page 7.

- If you deleted license and network settings, you must configure the appliance as if it were new, beginning with configuring it to communicate on your management network. For more information:
  - For Versions 5.4.x – 6.4.x, see Installation and Initial Setup for Versions 5.4 – 6.4.x, page 10.
  - For Versions 6.5+, see Installation and Initial Setup for Versions 6.5+, page 4.
- If you deregistered the Firepower Management Center from the Cisco Smart Software Manager, register the appliance to the Cisco Smart Software Manager. Choose **System > Licenses > Smart Licenses** and click the register icon.

After you complete the initial setup process:

- If you want to use a serial or SOL/LOM connection to access your appliance's console, you should redirect console output; see Redirecting Console Output, page 19.
- If LOM was reset during the restore and you want to use LOM, you must re-enable the feature as well as enable at least one LOM user; see Enabling LOM and LOM Users, page 37.

Setting Up Lights-Out Management

If you need to restore a Firepower device to factory defaults and do not have physical access to the appliance, you can use Lights-Out Management (LOM) to perform the restore process. Note that you can use Lights-Out Management on the default (`eth0`) management interface only.

The LOM feature allows you to perform a limited set of actions on a Firepower device, using a Serial over LAN (SOL) connection. With LOM, you use a command line interface on an out-of-band management connection to perform tasks such as viewing the chassis serial number, or monitoring conditions such as fan speed and temperature.

Caution: The Firepower Management Center 2000 and 4000 introduced Cisco's Unified Computing System (UCS) platform into the Firepower System. These models do not support Cisco functionality that uses tools on the baseboard management controller (BMC), such as the UCS Manager or the Cisco Integrated Management Controller (CIMC), to make any configuration changes or firmware updates.

The syntax of LOM commands depends on the utility you are using, but LOM commands generally contain the elements listed in the following table.

Table 5 LOM Command Syntax

IPMItool (Linux/Mac)	ipmiutil (Windows)	Description
ipmitool	ipmiutil	Invokes the IPMI utility.
n/a	-V4	For ipmiutil only, enables admin privileges for the LOM session.
-I lanplus	-J3	Enables encryption for the LOM session.
-H *IP_address*	-N *IP_address*	Specifies the IP address of the management interface on the appliance.

Table 5 LOM Command Syntax (continued)

IPMItool (Linux/Mac)	ipmiutil (Windows)	Description
-U *username*	-U *username*	Specifies the user name of an authorized LOM account.
n/a (prompted on login)	-P *password*	For ipmiutil only, specifies the password for an authorized LOM account.
command	command	The command you want to issue to the appliance. Note that where you issue the command depends on the utility: ■ For IPMItool, type the command last. ■ For ipmiutil, type the command first.

Therefore, for IPMItool:

```
ipmitool -I lanplus -H IP_address -U username command
```

Or, for ipmiutil:

```
ipmiutil command -V4 -J3 -N IP_address -U username -P password
```

Note that the `chassis power off` and `chassis power cycle` commands are not valid on 70xx Family appliances. For a full list of LOM commands supported by the Firepower System, see the Configuring Appliance Settings chapter in the *Firepower Management Center Configuration Guide*.

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.

Before you can restore an appliance using LOM, you must enable LOM for both the appliance and the user who will perform the restore. Then, use a third-party Intelligent Platform Management Interface (IPMI) utility to access the appliance. You must also make sure you redirect the appliance's console output to the serial port.

For more information, see the following sections:

- Enabling LOM and LOM Users, page 37
- Installing an IPMI Utility, page 38

Enabling LOM and LOM Users

Before you can use LOM to restore an appliance, you must enable and configure the feature. You must also explicitly grant LOM permissions to users who will use the feature.

You configure LOM and LOM users on a per-appliance basis using each appliance's local web interface. That is, you cannot use the Management Center to configure LOM on a Firepower device. Similarly, because users are managed independently per appliance, enabling or creating a LOM-enabled user on the Management Center does not transfer that capability to users on Firepower devices.

LOM users also have the following restrictions:

- You must assign the Administrator role to the user.
- The user name may have up to 16 alphanumeric characters. Hyphens and longer user names are not supported for LOM users.

- The password may have up to 20 alphanumeric characters. Longer passwords are not supported for LOM users. A user's LOM password is the same as that user's system password.
- Management Centers can have up to 13 LOM users.

Note: For detailed instructions on the following tasks, see the Configuring Appliance Settings chapter in the *Firepower Management Center Configuration Guide*.

To enable LOM:

1. Select **System > Configuration**, then click **Console Configuration**.
2. Enable remote access using the **Physical Serial Port** before you specify the LOM IP address, netmask, and default gateway (or use DHCP to have these values automatically assigned).

Note: The LOM IP address must be different from the management interface IP address of the appliance.

To enable LOM capabilities for a Firepower System user:

1. Select **System > User Management**, then either edit an existing user to add LOM permissions, or create a new user that you will use for LOM access to the appliance.
2. On the User Configuration page, enable the **Administrator** role if it is not already enabled.
3. Enable the **Allow Lights-Out Management Access** check box and save your changes.

Installing an IPMI Utility

You use a third-party IPMI utility on your computer to create an SOL connection to the appliance.

If your computer is running Linux or Mac OS, use IPMItool. Although IPMItool is standard with many Linux distributions, you must install IPMItool on a Mac. First, confirm that your Mac has Apple's xCode developer tools package installed. Also, make sure the optional components for command line development are installed (" UNIX Development" and " System Tools" in newer versions, or " Command Line Support" in older versions). Finally, install MacPorts and IPMItool. For more information, use your favorite search engine or see these sites:

```
https://developer.apple.com/technologies/tools/
http://www.macports.org/
```

For Windows environments, use ipmiutil, which you must compile yourself. If you do not have access to a compiler, you can use ipmiutil itself to compile. For more information, use your favorite search engine or see this site:

```
http://ipmiutil.sourceforge.net/
```

Preconfiguring Firepower Management Centers

You can preconfigure your Management Center 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.
- Shut down and ship the appliance to the target location.
- Deploy the appliances in the target locations.

Note: 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.

Note: 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.

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

Optional Preconfiguration Information

You can change some default configurations, such as:

- 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 3D7050 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 3D7050 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.

Preconfiguring Time Management

Keep in mind the following considerations:

- Cisco recommends that you synchronize time to a physical NTP server.
- 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 the *Firepower Management Center Configuration Guide* for more information.

Installing the System

Use the installation procedures described in Installation and Initial Setup for Versions 5.4 – 6.4.x, page 10 and Install the Appliance, page 11. For additional information, see the *Cisco Firepower Management Center 750, 1500, 2000, 3500, and 4000 Hardware Installation Guide*.

When preconfiguring the system, keep the following in mind:

- Add licenses for managed devices during the initial setup. If you do not add licenses at that time, any devices you register during initial setup are added to the Management Center as unlicensed; you must license each of them individually after the initial setup process is over. See License Settings, page 15.

Preparing the Appliance for Shipment

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

- To safely power down the appliance, see the *Cisco Firepower Management Center 1000, 2500, and 4500 Hardware Installation Guide*.
- To ensure that your appliance is safely prepared for shipping, see Shipping Considerations, page 40.

Deleting a License from a Management Center

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:

1. Select **Systems > Licenses**.
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.
3. Confirm that you want to delete the license.

   The license is deleted

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.
- 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: Management Centers, page 13.
- Confirm that the correct communication ports are functioning properly. See the documentation for your firewall for information on managing firewall ports. See the *Firepower Management Center Configuration Guide* for required open ports.

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

Scrubbing the Hard Drive

You can securely scrub the hard drive on Management Centers and Firepower devices to ensure that its contents can no longer be accessed. For example, if you need to return a defective appliance that contains sensitive data, you can use this feature to overwrite the data.

This mode of scrubbing the disk meets the following military standard:

> **STANDARDS**
>
> The DoD scrub sequence is compliant with the DoD 5220.22-M procedure for sanitizing removable and non-removable rigid disks which requires overwriting all addressable locations with a character, its complement, then a random character, and verify. Please refer to the DoD document for additional constraints.

Caution: Scrubbing your hard drive results in the loss of all data on the appliance, which is rendered inoperable.

You scrub the hard drive using an option in the interactive menu described in Using the Interactive Menu to Restore an Appliance, page 28.

To scrub the hard drive:

1. Follow the instructions in one of the following sections to display the restore utility's interactive menu, depending on how you are accessing the appliance:
   - Starting the Restore Utility Using KVM or Physical Serial Port, page 26
   - Starting the Restore Utility Using Lights-Out Management, page 27
2. From the restore utility main menu, select **8 Wipe Contents of Disk**.
3. When prompted, confirm that you want to scrub the hard drive.

The hard drive is scrubbed. The scrub process may take several hours to complete; larger drives take longer.

Related Documentation

For a complete list of the Cisco Firepower Management Center series documentation and where to find it, see the documentation roadmap at the following URL:

https://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html