

# **Restoring a Firepower System Appliance to Factory Defaults**

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

For more information, see the following sections:

- Before You Begin, page 8-1
- Understanding the Restore Process, page 8-2
- Obtaining the Restore ISO and Update Files, page 8-3
- Beginning the Restore Process, page 8-4
- Using the Interactive Menu to Restore an Appliance, page 8-6
- Next Steps, page 8-14
- Setting Up Lights-Out Management, page 8-15

## **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.

### **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, console, and Lights-Out Management (LOM) settings, you must perform all other setup tasks after the restore process completes.

### **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**

#### Access: Admin

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 8-1.

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. For more information, including a table of serial port connectors by appliance, see Serial Connection/Laptop, page 4-20.

#### 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 (etho) management interface only. For more information, see Setting Up Lights-Out Management, page 8-15.

#### **Before You Begin**

 Obtain the restore ISO image for the appliance from the Support Site. See To obtain the restore ISO and other update files:, page 8-3

#### To restore a Firepower device:

- **Step 1** Copy the image to an appropriate storage medium.
- **Step 2** Connect to the appliance.
- **Step 3** Reboot the appliance and invoke the restore utility.

#### What to Do Next

• Install the ISO image using the procedure in To restore a Firepower device:, page 8-2.

## **Obtaining the Restore ISO and Update Files**

#### Access: Any

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:

- **Step 1** Using the user name and password for your support account, log into the Support Site (https://sso.cisco.com/autho/forms/CDClogin.html).
- **Step 2** Browse to the software download section (https://software.cisco.com/download/navigator.html).
- **Step 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**.

**Step 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 **5.4.1 Images** to view the images and release notes for Version 5.4.1 of the Firepower System.

Step 5 Click the ISO image you want to download.

The file begins downloading.

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

If using FTP, the user name and password must be associated with an account on the FTP server. If you are writing to the server, the FTP server must be properly configured to accept the FTP write request from the user. Refer to the documentation for your FTP server for more information.



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 8-4 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 8-5 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 on a Firepower device, 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

Access: Admin

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



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 8-5.

#### To start the restore utility:

**Step 1** Using your keyboard/monitor or serial connection, log into the appliance using an account with Administrator privileges. The password is the same as the password for the appliance's web interface.

- **Step 2** Reboot the appliance:
  - On a Firepower device, type system reboot.

The appliance reboots.

**Step 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 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). The LILO boot prompt appears. For example:

```
LILO 22.8 boot:
System-5.4 System Restore
```

- **Step 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 connection, type System\_Restore at the prompt and press Enter.

The boot prompt appears after the following choices:

- 0. Load with standard console
- 1. Load with serial console
- **Step 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 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.

**Step 6** Press Enter to confirm the copyright notice.

#### What to Do Next

• Continue with Using the Interactive Menu to Restore an Appliance, page 8-6.

### Starting the Restore Utility Using Lights-Out Management

#### Access: Admin

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 if you want to use LOM to configure the initial setup, you **must** preserve the network settings during the initial setup. Note also that you can use Lights-Out Management on the default (etho) management interface only.



Before you can restore an appliance using LOM, you must enable the feature; see Setting Up Lights-Out Management, page 8-15.

To start the restore utility using Lights-Out Management:

**Step 1** 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.

If you are using a Firepower device, type expert to display the shell prompt.

- **Step 2** Reboot the appliance as root user:
  - For a Firepower device, type system reboot.

The appliance reboots.

**Step 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.

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:

LILO 22.8 boot: System-5.4 System\_Restore

Step 4 At the boot prompt, start the restore utility by typing System\_Restore.

The boot prompt appears after the following choices:

Load with standard console
 Load with serial console

**Step 5** 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.

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.

**Step 6** Press Enter to confirm the copyright notice.

#### What to Do Next

• Continue with Using the Interactive Menu to Restore an Appliance, page 8-6.

## Using the Interactive Menu to Restore an Appliance

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

# <u>Note</u>

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 8-1.

The menu displays the options listed in the following table.

#### Table 8-1Restore 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 8-8	
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 8-9	
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 8-10	
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 8-11	
5 Run the Install	Invoke the restore process.	Invoking the Restore Process, page 8-11	
6 Save Configuration	Save any set of restore configurations for later use,	Saving and Loading Restore	
7 Load Configuration	or load a saved set.	Configurations, page 8-13	
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 D-1	

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 8-11. However, Cisco recommends you double-check the settings in the restore configuration before proceeding.

 $\mathcal{P}$ 

Тір	To use a previously saved configuration, start with menu option <b>6</b> : Saving and Loading Restore Configurations, page 8-13. After you load the configuration, skip to menu option <b>4</b> : Downloading the ISO and Update Files and Mounting the Image, page 8-11.		
	To restore an appliance using the interactive menu, use the following steps:		
Step 1	<b>1 IP Configuration</b> — see Identifying the Appliance's Management Interface, page 8-8.		
Step 2	2 Choose the transport protocol — see Specifying ISO Image Location and Transport Method, page 8-9.		
Step 3	<b>3 Select Patches/Rule Updates</b> (optional) — Updating System Software and Intrusion Rules During Restore, page 8-10.		
Step 4	<b>4 Download and Mount ISO</b> — see Downloading the ISO and Update Files and Mounting the Image, page 8-11.		
Step 5	<b>5 Run the Install</b> — see Invoking the Restore Process, page 8-11.		

## Identifying the Appliance's Management Interface

#### Access: Admin

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:

Step 1	From the main menu, select 1 IP Configuration.	
Step 2	Select the appliance's management interface (generally eth0).	
Step 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.	
Step 4	Select a method to assign an IP address to the management interface: Static or DHCP:	
	• If you select <b>Static</b> , 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 <b>DHCP</b> , the appliance automatically detects the IP address, network mask or prefix length, and default gateway for the management interface, then displays the IP address.	
Step 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.

1

8-9

### Specifying ISO Image Location and Transport Method

#### Access: Admin

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 8-3), 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.

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			
	<b>Note</b> The FTP protocol requires a client to send a remote user name and password on each FTP request to a server. The user name and password must be associated with an account on the FTP server. If you are writing to the server, the FTP server must be properly configured to accept the FTP write request from the user. Refer to the documentation for your FTP server for more information.			
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			
	<b>Note</b> 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.			

Table 8-2 Information Needed to Download Restore Files

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:

- Step 1 From the main menu, select **2** Choose the transport protocol.
- On the page that appears, select either HTTP, FTP, or SCP. Step 2

If using FTP, the user name and password must be associated with an account on the FTP server. If you are writing to the server, the FTP server must be properly configured to accept the FTP write request from the user. Refer to the documentation for your FTP server for more information.

Step 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 8-2 on page 8-9.

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.

- **Step 4** Select the ISO image you want to use.
- **Step 5** When prompted, confirm your settings.
- **Step 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 8-11. 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

#### Access: Admin

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 8-3.

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:

Step 1 From the 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 8-9) 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.

**Step 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.

**Step 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**

#### Access: Admin

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 8-13.

#### To download and mount the ISO image:

- Step 1 From the main menu, select 4 Download and Mount ISO.
- **Step 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**

#### Access: Admin

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.



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 8-12.

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

- Step 1 From the main menu, select 5 Run the Install.
- **Step 2** When prompted (twice), confirm that you want to reboot the appliance.
- **Step 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:

LILO 22.8 boot:

System-5.4 System\_Restore

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

**Step 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.

**Step 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 8-6.

#### **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:

- Step 1 From the main menu, select 5 Run the Install.
- **Step 2** Confirm that you want to restore the appliance and continue with the next step.
- **Step 3** Choose whether you want to delete the appliance's license and network settings. Deleting these settings also resets display (console) and LOM 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 8-14.



**Caution** Do **not** delete the network settings if you are restoring the appliance using a LOM connection. After you reboot the appliance, you will be unable to reconnect via LOM.

**Step 4** 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.

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 8-1.

#### What to Do Next

• Continue with Next Steps, page 8-14.

### Saving and Loading Restore Configurations

#### Access: Admin

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 8-8
- 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 8-9
- 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 8-10

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:

- Step 1 From the restore utility's main menu, select 6 Save Configuration.The utility displays the settings in the configuration you are saving.
- **Step 2** When prompted, confirm that you want to save the configuration.

**Step 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 8-11.

#### To load a saved restore configuration:

Step 1 From the 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.

**Step 2** Select the configuration you want to use.

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

**Step 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 8-11.

## **Next Steps**

Restoring your appliance to factory default settings results in the loss of almost **all** configuration and event data on the appliance, including bypass configurations for devices deployed inline. For more information, see Traffic Flow During the Restore Process, page 8-1.

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, see Initial Setup Page: Firepower Devices, page 5-5.
- 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. See Setting Up Firepower Managed Devices, page 5-1.

Note that deleting license and network settings also resets display (console) and LOM settings=. 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 Testing an Inline Bypass Interface Installation, page 4-24.
- If 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 8-16.

# **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 (etho) management interface only.

Note

The baseboard management controller (BMC) for a Firepower 71xx, Firepower 82xx, or a Firepower or AMP 83xx device is only accessible via 1Gbps link speeds when the host is powered on. When the device is powered down the BMC can only establish Ethernet link at 10 and 100Mbps. Therefore if LOM is being used to remotely power the device, connect the device to the network using 10 and 100Mbps link speeds 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.

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

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.
-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.

Table 8-3LOM Command Syntax

#### 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*.

<u>Note</u>

Before you can connect to a 7000 Series device using SOL, you must disable Spanning Tree Protocol (STP) on any third-party switching equipment connected to the device's management interface.

<u>Note</u>

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 8-16
- Installing an IPMI Utility, page 8-17

## **Enabling LOM and LOM Users**

#### Access: Admin

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 and 8000 Series devices can have up to 13 LOM users. 7000 Series devices can have up to eight LOM users.



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

#### To enable LOM:

- Step 1 Select System > Configuration, then click Console Configuration.
- **Step 2** Your next step depends on your appliance model:

- To enable LOM on Firepower 8000 Series devices, you must enable remote access using the Physical Serial Port before you can specify the LOM IP address, netmask, and default gateway (or use DHCP to have these values automatically assigned).
- On Firepower 7000 Series devices, select Lights Out Management to configure LOM settings. 7000 Series devices do not support LOM and physical serial access at the same time.

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:

- **Step 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.
- **Step 2** On the User Configuration page, enable the **Administrator** role if it is not already enabled.
- Step 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/



1

