Cisco Firepower 7000 Series Getting Started Guide

For the 70x0 and 71xx Firepower and AMP models

Updated: August 22, 2018

This guide is organized as follows:

Package Contents

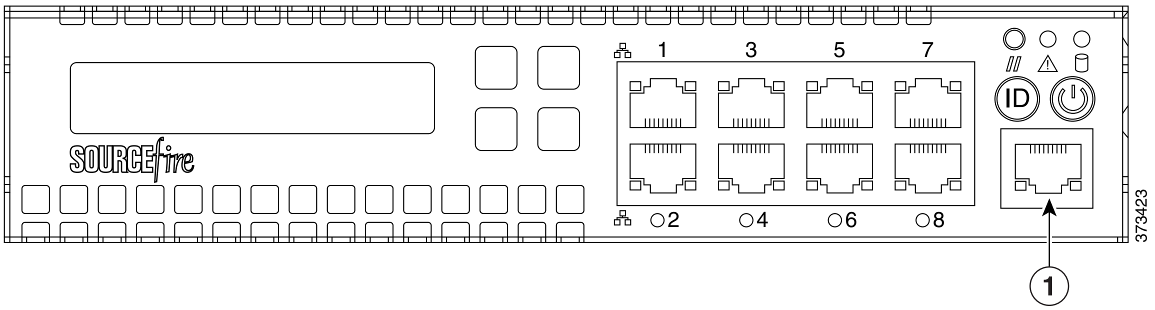
This section lists the items included with each model. Note that contents are subject to change, and your exact contents might contain additional or fewer items.

Chassis Models

A Firepower 7000 Series device can be delivered on a variety of chassis:

- Firepower 7010/7020/7030/7050 are 1U appliances that are one-half the width of the chassis tray. The following illustration of the front of the chassis indicates the management interface.

Figure 1 Firepower 70x0 Series Chassis and Management Interface

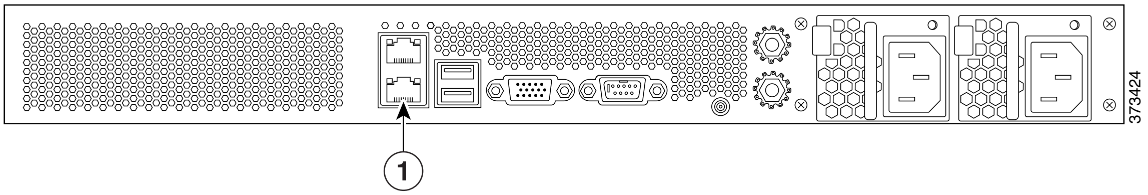


1	Management Interface		

Cisco Systems, Inc. www.cisco.com

- The Firepower 7110/7120/7115/7125, and the AMP7150 are available as 1U appliances. The following illustration of the rear of the chassis indicates the location of the management interface.

Figure 2 Firepower and AMP 71xx Series Chassis and Management Interface



1	Management interface		

Included Items

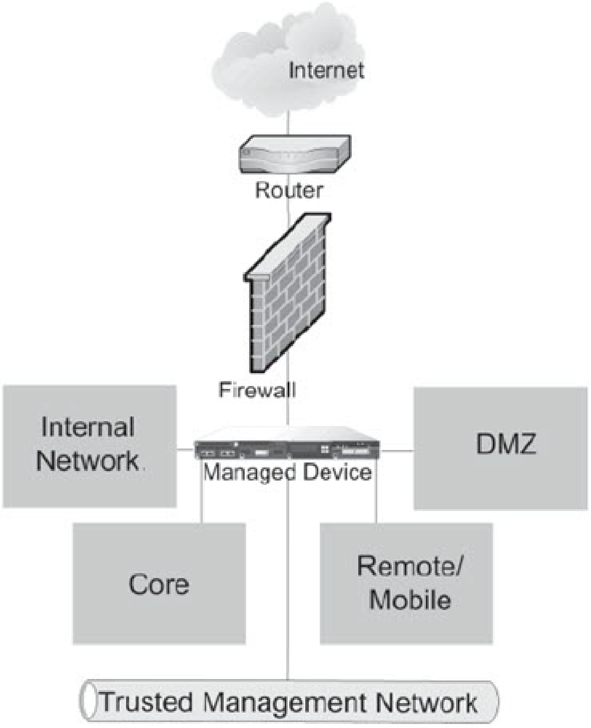
- One power cords per chassis (Firepower 70x0 Series).
- Two power cords per chassis (Firepower and AMP 71xx Series).
- Two straight-through Cat 5e Ethernet cables.
- One rack-mounting kit per chassis.

Note: Each model group has identical chassis. If you are not sure which model you have, see your packing list.

Required Items

- Flathead and Phillips screwdrivers for the rack-mounting kit.
- Firepower 7010/7020/7030/7050 only: chassis tray, available separately
- Firepower 7115/7125, AMP7150 only: small form-factor pluggable (SFP) transceivers, available separately (optional)

Deploying the Appliance



Your device is typically deployed inside a firewall, where it is connected to your trusted management network and the various network segments you want to monitor.

In a simple deployment scenario, you connect the management interface on your device to your trusted management network using an Ethernet cable, then connect the sensing interfaces to the network segments you want to monitor using the appropriate cables (copper or fiber) in either a passive or inline cabling configuration.

The trusted management network (a restricted network protected from unauthorized access) may have a single secure connection to the Internet for security updates and similar functions, but is separate from the rest of your network and is not accessible to hosts used in daily business operations.

You can connect sensing interfaces to different network segments dedicated to particular components of your business that have distinct security requirements to target policies based on the needs for specific segments. These segments can include the DMZ (outward-facing servers, such as mail, ftp, and web hosts), your internal network (hosts used in daily operation and similar applications), and the core (hosts reserved for critical business assets), and can also include segments dedicated to remote locations, mobile access, or other functions.

How you cable your sensing interfaces determines your configuration options. If you use passive cabling, you can configure passive sensing interfaces. If you use inline cabling, you can create passive, inline, inline with fail-open, virtual switch, virtual router, or hybrid sensing interfaces on your device. For more information on deployment options and interface configurations and how they affect product features, see the *Firepower Firepower Management Center Configuration Guide* and the *Firepower 8000 Series Hardware Installation Guide*.

Cabling the Device

You can cable your device to configure passive or inline interfaces, depending on your deployment needs.

Use passive cabling if you want to:

- monitor traffic
- collect information about hosts, operating systems, applications, users, files, networks, and vulnerabilities

Use inline cabling if you want to use the same features as a passive deployment, plus:

- configure a virtual switch, virtual router, or hybrid interface
- perform network address translation (NAT)
- use policies to block traffic based on access control features such as application control, user control, security intelligence, URL dispositions, file control, malware detection, or intrusion prevention

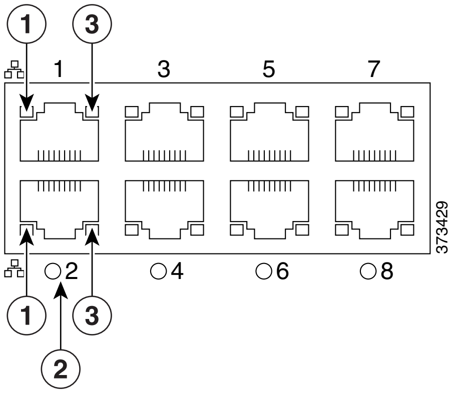
Use the appropriate cables (as indicated by your interface) and cabling diagram for the interface you want to configure, then use the web interface on the Firepower Management Center to configure the interfaces. See Connecting the Sensing Interfaces, page 7.

Understanding the Sensing Interfaces

Firepower 7010/7020/7030/7050

The Firepower 7010/7020/7030/7050 is a 1U device one-half the width of the rack tray with eight copper sensing interfaces, each with bypass capability.

Figure 3 Eight Copper Sensing Interfaces



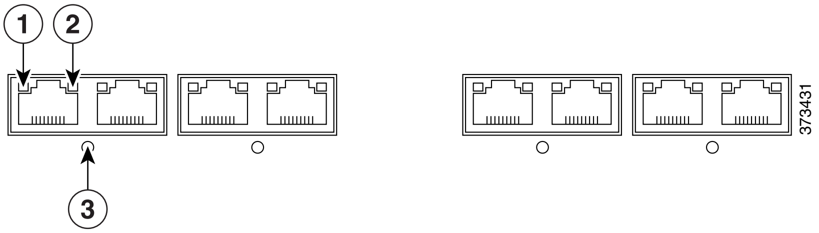
1	Link LED	**3**	Activity LED
2	Bypass LED		

You can use these interfaces to passively monitor up to eight separate network segments. You can also use paired interfaces in an inline configuration on up to four network segments.

Firepower 7110/7120

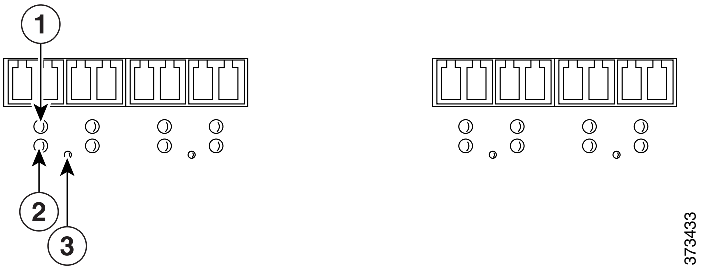
The Firepower 7110/7120 is a 1U device with eight copper or eight fiber sensing interfaces, each with bypass capability.

Figure 4 Eight 1000BASE-T Copper Sensing Interfaces



1	Link LED	**3**	Bypass LED
2	Activity LED		

Figure 5 Eight 1000BASE-SX Fiber Sensing Interfaces



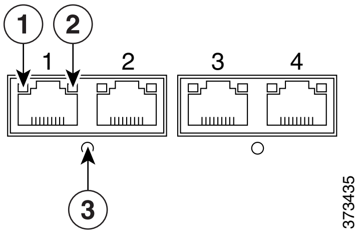
1	Link LED	**3**	Bypass LED
2	Activity LED		

You can use these interfaces to passively monitor up to eight separate network segments. You can also use paired interfaces in an inline configuration on up to four network segments.

Firepower 7115/7125, AMP7150

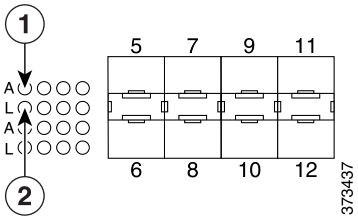
The Firepower 7115/7125 and AMP7150 are 1U devices with four copper sensing interfaces with bypass capability and eight small form-factor pluggable (SFP) sockets without bypass capability.

Figure 6



1	Link LED	**3**	Bypass LED
2	Activity LED		

Figure 7

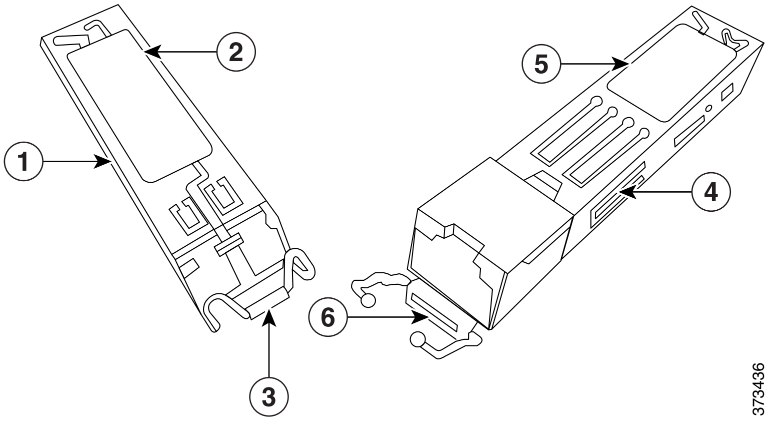


1	Activity LED	**2**	Link LED

You can use the four copper interfaces to passively monitor up to four separate network segments. You can also use paired interfaces in an inline configuration on up to two network segments.

You can insert up to eight SFP transceivers (any combination of copper, fiber, or both) and use their interfaces to monitor up to eight separate network segments. You can also use any combination of transceivers on sequentially paired interfaces (interfaces 5 and 6, 7 and 8, 9 and 10, or 11 and 12) in an inline deployment. Note that SFP interfaces do not have bypass capabilities.

Figure 8



1	Fiber SFP sample	**4**	Copper SFP sample
2	Fiber rear with contacts	**5**	Copper rear with contacts
3	Fiber front with bale	**6**	Copper front with bale

Inserting or Removing a Small Form-Factor Pluggable (SFP) Transceiver

The Firepower 7115/7125 and AMP7150 contain eight SFP sockets in a “tab toward center” configuration. Cable the interface on the transceiver after the transceiver is inserted into the chassis.

Use appropriate electrostatic discharge (ESD) procedures when inserting or removing the transceiver. Avoid touching the contacts, and keep the contacts and interfaces free of dust and dirt.

Caution: Do not force an SFP transceiver into a socket as this can jam the transceiver and can cause permanent damage to the transceiver, the chassis, or both. Use only approved SFP tranceivers. Non-Cisco transceivers may jam in the socket and can cause permanent damage to the transceiver, the chassis, or both.

To insert an SFP transceiver into the chassis SFP socket:

1. Taking care not to touch the contacts in the rear, use your fingers to grasp the sides of the bale and slide the rear of the transceiver into a socket on the chassis. Note that sockets on the upper row face up and sockets on the lower row face down.
2. Gently push the bale toward the transceiver to engage the locking mechanism, securing the transceiver in place.

To remove an SFP transceiver:

1. Disconnect all cables from the transceiver you want to remove from the device.
2. Using your fingers, gently pull the bale of the transceiver away from the chassis to disengage the locking mechanism.

   For transceivers in the upper row, pull down. For transceivers in the lower row, lift up.
3. Gently slide the transceiver directly out of the socket, taking care not to touch the contacts at the back of the transceiver.

   If the transceiver does not slide out easily, push the transceiver back into the socket and try again, using the bale as a handle.

Connecting the Sensing Interfaces

After you cable the interfaces, use the web interface on the Firepower Management Center that manages the device to configure the device's sensing interfaces as passive, inline, inline with fail-open, switched, routed, or hybrid. Use only the interfaces on the front of the device as sensing interfaces.

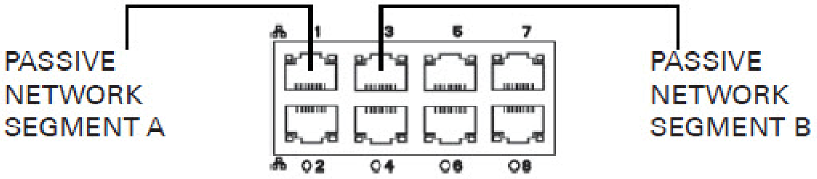
See the *Firepower 7000 Series Hardware Installation Guide* for detailed information on planning your deployment. After you have selected a deployment model, cable the sensing interfaces as needed for your configuration.

Passive Interface Cabling

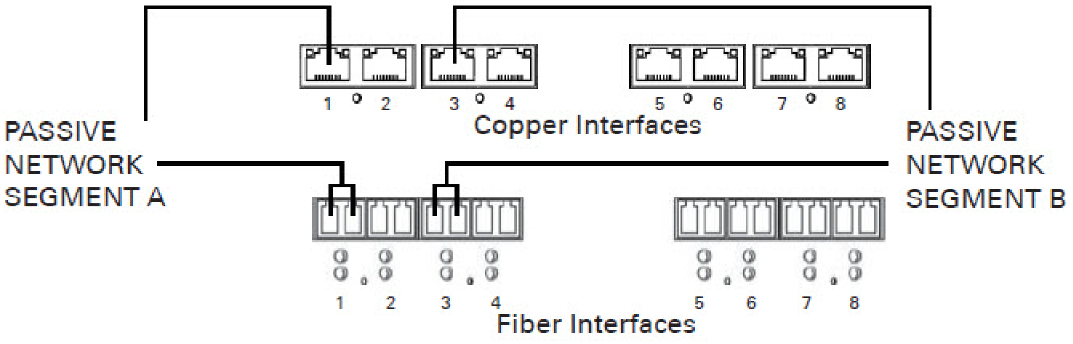
For each network segment you want to monitor passively, connect the appropriate cables (either fiber or copper) to one sensing interface.

Use this cabling when you want to configure passive interfaces.

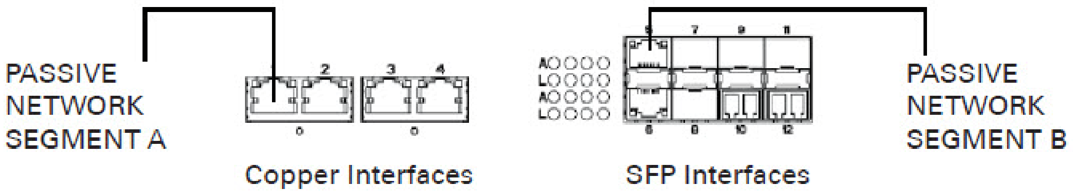
Firepower 7010/7020/7030/7050



Firepower 7110/7120



Firepower 7115/7125, AMP7150

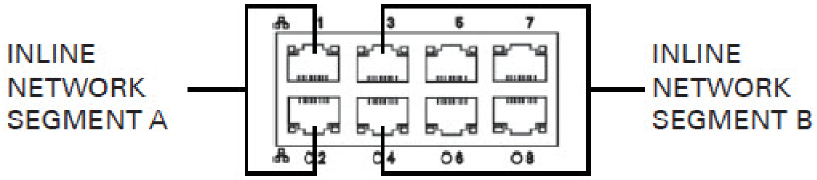


Inline Interface Cabling

For each network segment you want to monitor inline, connect the appropriate cables (either copper or fiber sequentially to pairs of sensing interfaces.

Use this cabling when you want to configure inline, inline with fail-open, switched, routed, or hybrid interfaces.

Firepower 7010/7020/7030/7050

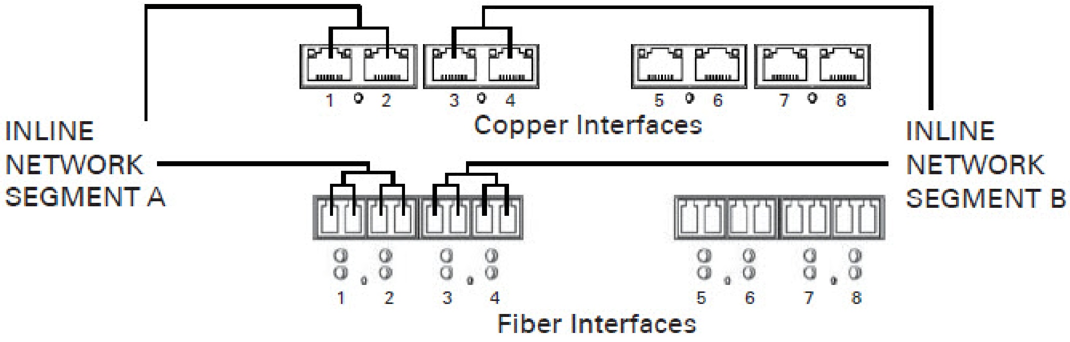


Inline with Fail-Open Configuration

If you want to take advantage of the device's configurable fail-open capability, you must cable a sequential pair of vertical interfaces (interfaces 1 and 2, 3 and 4, 5 and 6, or 7 and 8) to a network segment.

After you cable the interfaces, use the web interface on the Defense Center that manages the device to configure the interface as inline with fail-open. See Setting Up an IPS Device in the *Firepower Management Center Configuration Guide*.

Firepower 7110/7120

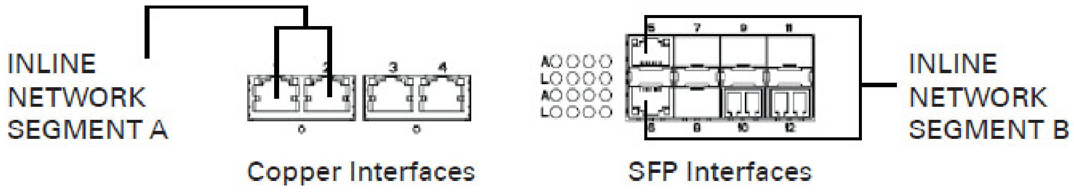


Inline with Fail-Open Configuration

If you want to take advantage of the device's configurable fail-open capability, you must cable a sequential pair of interfaces (interfaces 1 and 2, 3 and 4, 5 and 6, or 7 and 8) to a network segment.

After you cable the interfaces, use the web interface on the Defense Center that manages the device to configure the interface as inline with fail-open. See Setting Up an IPS Device in the *Firepower Management Center Configuration Guide*.

Firepower 7115/7125, AMP7150



Inline with Fail-Open Configuration

You can configure SFP interfaces inline, but SFP interfaces do not have inline fail-open capability. If you want to take advantage of the device's configurable fail-open capability, you must cable a sequential pair of copper interfaces (interfaces 1 and 2, or 3 and 4) to a network segment.

After you cable the interfaces, use the web interface on the Defense Center that manages the device to configure the interface as inline with fail-open. See Setting Up an IPS Device in the *Firepower Management Center Configuration Guide*.

Installing the Firepower 7000 Series Device

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, a serial connection, or using an Ethernet connection to the management interface.

Note: The management interface is pre-configured with a default IPv4 address. However, you can reconfigure the management interface with an IPv6 address as part of the setup process.

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.

Serial Connection

You can connect a computer to any 7000 Series appliance using the physical serial port. Connect the appropriate rollover serial cable (also known as a NULL modem cable or Cisco console cable) at any time, then configure the remote management console to redirect the default VGA output to the serial port. To interact with the appliance, use terminal emulation software such as HyperTerminal or XModem. The settings for this software are 9600 baud, 8 data bits, no parity checking, 1 stop bit, and no flow control.

Ethernet Connection to Management Interface

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

Using an Ethernet cable, connect the network interface on the local computer to the management interface on the appliance. Note that the 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.

To install the appliance:

1. Mount the appliance in your rack using the mounting kit and its supplied instructions.
2. Connect to the appliance using either a keyboard and monitor or an Ethernet connection.
   - If you are using a keyboard and monitor to set up the appliance, use an Ethernet cable now to connect the management interface to a protected network segment.
   - If you plan to perform the initial setup process by connecting a computer directly to the appliance's physical management interface, you will connect the management interface to the protected network when you finish setup.
3. Connect the sensing interfaces to the network segments you want to analyze using the appropriate cables for your interfaces:
   - Copper Sensing Interfaces: If your device includes copper sensing interfaces, make sure you use the appropriate cables to connect them to your network; see Cabling Inline Deployments on Copper Interfaces in the Firepower 8000 Series Hardware Installation Guide.
   - Fiber Adapter Card: For devices with a fiber adapter card, connect the LC connectors on the optional multimode fiber cable to two ports on the adapter card in any order. Connect the SC plug to the network segment you want to analyze.
   - Fiber Tap: If you are deploying the device with an optional fiber optic tap, connect the SC plug on the optional multimode fiber cable to the "analyzer" port on the tap. Connect the tap to the network segment you want to analyze.
   - Copper Tap: If you are deploying the device with an optional copper tap, connect the A and B ports on the left of the tap to the network segment you want to analyze. Connect the A and B ports on the right of the tap (the "analyzer" ports) to two copper ports on the adapter card.

   For more information about options for deploying the managed device, see Deploying Managed Devices in the Firepower 8000 Series Hardware Installation Guide.

   Note that if you are deploying a device with bypass interfaces, you are taking advantage of your device's ability to maintain network connectivity even if the device fails. See Testing an Inline Bypass Interface Installation in the Firepower 8000 Series Hardware Installation Guide for information on installation and latency testing.
4. 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.
5. Turn on the appliance.
6. If you are using a direct Ethernet connection to set up 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.

   If the management interface and network interface LEDs are not lit, try using a crossover cable. For more information, see Cabling Inline Deployments on Copper Interfaces in the Firepower 8000 Series Hardware Installation Guide.

What to Do Next

- Complete the setup process using the procedures in Initial Device Setup, page 11.

Initial Device Setup

After you deploy and install a new Firepower device, you must complete a setup process. The setup process also allows you to perform many initial administrative-level tasks, such as setting the time, registering and licensing devices, 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.

Before you begin the setup, make sure that you can meet the following conditions:

Access

To set up a new appliance, you must connect using either keyboard and monitor/KVM or a direct Ethernet connection to the appliance's management interface. After initial setup, you can configure the appliance for serial access. For more information, see "Rack-Mounting a Firepower Device" in the *Firepower 8000 Series Hardware Installation Guide*.

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.

Network and Deployment Information

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, and a default gateway.

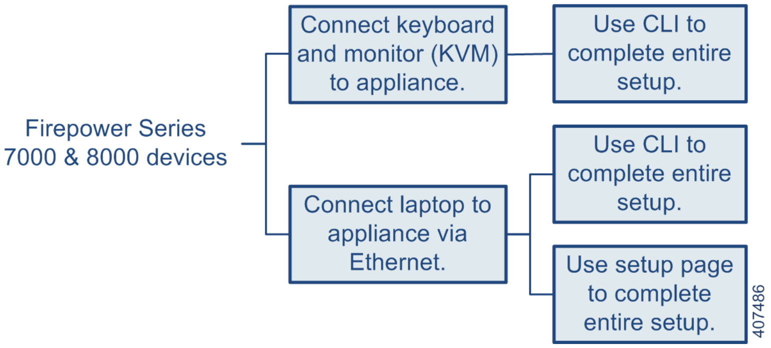
If you know how the appliance is deployed, the setup process is also a good time to perform many initial administrative-level tasks, including registration and licensing.

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 Firepower Management Center; the setup process for a Firepower Management Center allows you to add and license preregistered managed devices.

After you complete setup, you will use the Firepower Management Center's web interface to perform most management and analysis tasks for your deployment. Firepower devices have a restricted web interface that you can use only to perform basic administration. For more information, see Next Steps, page 17.

Note: If you are setting up an appliance after restoring it to factory defaults (see Restoring a Device to Factory Defaults, page 19) 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 Using the Web Interface, page 12.

The following diagram illustrates the choices you can make when setting up Firepower devices:


Firepower Series 7000 & 8000 devices
Connect keyboard and monitor (KVM) to appliance.
Use CLI to complete entire setup.
Connect laptop to appliance via Ethernet.
Use CLI to complete entire setup.
Use setup page to complete entire setup.
407486

Your access to a Firepower device determines how you set it up. You have the following options:

- If you are accessing the appliance via a direct Ethernet connection, you can browse to the appliance's web interface from a local computer; see Initial Setup Using the Web Interface, page 12.

- Regardless of how you are connected to the device, you can use the CLI to set it up; see Initial Setup Using the CLI, page 15.

If you are setting up a reimaged device and you kept your network settings as part of the restore process, you can access the CLI via SSH or a Lights-Out Management (LOM) connection. You can also browse to the device's web interface from a computer on your management network.

Caution: The procedures in this guide explain how to set up an appliance without powering it down. However, if you need to power down for any reason, use the procedure in the Device Management Basics chapter in the *Firepower Management Center Configuration Guide*, 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).

Initial Setup Using the Web Interface

In most cases, complete the setup process by logging into the device's web interface and specifying initial configuration options on a setup page.

Procedure

1. Direct your browser to `https://`*`mgmt_ip`*`/`, where *`mgmt_ip`* is the IP address of the device's management interface.
   - For a device 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 device where network settings are already configured, use a computer on your management network to browse to the IP address of the device's management interface.
2. Log in using `admin` as the username and `Admin123` as the password.

   See the following sections for information on initial setup options:
   - Change Password, page 13
   - Network Settings, page 13
   - Firepower Device LCD Panel Configuration, page 13
   - Remote Management, page 13
   - Time Settings, page 13
   - Detection Mode, page 14
   - Automatic Backups, page 15
   - End User License Agreement, page 15
3. When you are finished, click **Apply**.

   The device is configured according to your selections. You are logged into the web interface as the `admin` user, which has the Administrator role.
4. Log out of the device.

   The device is ready to be added to its Firepower Management Center.

   Note: If you connected directly to the device using an Ethernet cable, disconnect the computer and connect the device's management interface to the management network. If you need to access the device's web interface at any time, direct a browser on a computer on the management network to the IP address or host name that you configured during setup.

Change Password

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

This password allows the `admin` user to log into the device's web interface and its CLI; the `admin` user has Configuration CLI access. Changing any user's password for the web interface also changes the password for the CLI, and vice versa.

Network Settings

A device's network settings allow it to communicate on your management network. If you already configured the device's 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.

Firepower Device LCD Panel Configuration

Select whether you want to allow changing of a Firepower device's network settings using the LCD panel.

Note: Enabling this option can represent a security risk. You need only physical access, not authentication, to configure network settings using the LCD panel. For more information, see "Using the LCD Panel on a Firepower Device" in the *Firepower 8000 Series Hardware Installation Guide*.

Remote Management

You must manage a Cisco device with a Firepower Management Center. In this two-step process, you first configure remote management on the device, then add the device to a Firepower Management Center. For your convenience, the setup page allows you to preregister the device to the Firepower Management Center that will manage it.

Leave the **Register This Device Now** check box enabled, then specify the IP address or fully qualified domain name of the managing Firepower Management Center as the **Management Host**. Also, type the alphanumeric **Registration Key** you will later use to register the device to the Firepower Management Center. Note that this is a simple key that you specify, up to 37 characters in length, and is not the same as the license key.

If the device and Firepower Management Center are separated by a network address translation (NAT) device, defer device registration until after you complete the initial setup. See the Managing Devices chapter in the *Firepower Management Center Configuration Guide* for more information.

Time Settings

You can set the time for a device either manually or via network time protocol (NTP) from an NTP server, including the Firepower Management Center. Cisco recommends that you use the Firepower Management Center as the NTP server for its managed devices.

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.

Detection Mode

The detection mode you choose for a device determines how the system initially configures the device's interfaces, and whether those interfaces belong to an inline set or security zone.

The detection mode is not a setting you can change later; it is simply an option you choose during setup that helps the system tailor the device's initial configurations. In general, you should choose a detection mode based on how your device is deployed:

- **Passive** - choose this mode if your device is deployed passively, as an intrusion detection system (IDS). In a passive deployment, you can perform file and malware detection, Security Intelligence monitoring, as well as network discovery.
- **Inline** - choose this mode if your device is deployed inline, as an intrusion prevention system. An intrusion prevention system usually fails *open* and *allows* non-matching traffic.

  In an inline deployment, you can also use AMP for Networks, file control, Security Intelligence filtering, and network discovery.

Note: Reimaging resets devices in inline deployments to a non-bypass configuration; this disrupts traffic on your network until you reconfigure bypass mode. For more information, see Traffic Flow During the Restore Process, page 19.

- **Access Control** - choose this mode if your device is deployed inline as part of an access control deployment, that is, if you want to perform application, user, and URL control. A device configured to perform access control usually fails *closed* and *blocks* non-matching traffic. Rules explicitly specify the traffic to pass.

  You should also choose this mode if you want to take advantage of your device's specific hardware-based capabilities, which include (depending on model): high availability, strict TCP enforcement, fast-path rules, switching, routing, DHCP, NAT, and VPN.

  In an access control deployment, you can also perform AMP for Networks, file control, Security Intelligence filtering, and network discovery.
- **Network Discovery** - choose this mode if your device is deployed passively, to perform host, application, and user discovery only.

The following table lists the interfaces, inline sets, and zones that the system creates depending on the detection mode you choose.

Table 1 Initial Configurations Based on Detection Mode

Detection Mode	Security Zones	Inline Sets	Interfaces
Inline	Internal and External	Default Inline Set	first pair added to Default Inline Set—one to the Internal and one to the External zone
Passive	Passive	none	first pair assigned to Passive zone
Access Control	none	none	none
Network Discovery	Passive	none	first pair assigned to Passive zone

Note: Security zones are a Firepower Management Center-level configuration which the system does not create until you actually register the device to the Firepower Management Center. Upon registration, if the appropriate zone (Internal, External, or Passive) already exists on the Firepower Management Center, the registration process adds the listed interfaces to the existing zone. If the zone does not exist, the system creates it and adds the interfaces. For detailed information on interfaces, inline sets, and security zones, see the *Firepower Management Center Configuration Guide*.

Automatic Backups

The device provides a mechanism for archiving data so that configuration and event data 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 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 device is configured according to your selections and is ready to be added to its managing Firepower Management Center.

Initial Setup Using the CLI

Optionally, you can use the CLI to configure Firepower devices instead of using the device's web interface.

Note that the CLI prompts you for much of the same setup information that a device's setup web page does. For detailed information on these options, see Initial Setup Using the Web Interface, page 12.

Procedure:

1. Log into the device. Use `admin` as the username and `Admin123` as the password.

   – For a device attached to a monitor and keyboard, log in at the console.

   – If you connected a computer to the management interface of the device using an Ethernet cable, SSH to the interface's default IPv4 address: 192.168.45.45.

   The device immediately prompts you to read the EULA.

2. Read and accept the EULA.

3. Change the password for the `admin` account. This account has Administrator privileges and cannot be deleted.

   This password allows the `admin` user to log into the device's web interface and its CLI; the `admin` user has Configuration CLI access. Changing any user's password for the web interface also changes the password for the CLI, and vice versa.

   Cisco recommends that you use 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. For more information, see Change Password, page 13.

4. Configure network settings for the device.

   First configure (or disable) IPv4 management settings, then IPv6. If you manually specify network settings, you must:

   – enter IPv4 addresses, including the netmask, in dotted decimal form. For example, you could specify a netmask of 255.255.0.0.

   – enter IPv6 addresses in colon-separated hexadecimal form. For an IPv6 prefix, specify the number of bits; for example, a prefix length of 112.

   For more information, see Network Settings, page 13. The console may display messages as your settings are implemented.

5. Select whether you want to allow changing of the device's network settings using the LCD panel.

Caution: Enabling this option can present a security risk. You need only physical access, not authentication, to configure network settings using the LCD panel. For more information, see the *Firepower 8000 Series Hardware Installation Guide*.

6. Specify the detection mode based on how you deployed the device.

   For more information, see Detection Mode, page 14. The console may display messages as your settings are implemented. When finished, the device reminds you to register this device to a Firepower Management Center, and displays the CLI prompt.

7. To use the CLI to register the device to the Firepower Management Center that will manage it, continue with the next section, Register a Firepower Device to a Management Center Using the CLI.

   You must manage devices with a Firepower Management Center. If you do not register the device now, you must log in later and register it before you can add it to a Firepower Management Center.

8. Log out of the device.

Register a Firepower Device to a Management Center Using the CLI

If you configured a Firepower device using the CLI, Cisco recommends that you use the CLI to register the device to a Firepower Management Center at the conclusion of the setup script. It is easiest to register a device to its Firepower Management Center during the initial setup process, because you are already logged into the device's CLI.

To register a device, use the `configure manager add` command. A unique alphanumeric registration key is always required to register a device to a Firepower Management Center. This is a simple key that you specify, up to 37 characters in length, and is not the same as a license key.

In most cases, you must provide the Firepower Management Center's hostname or the IP address along with the registration key, for example:

```
configure manager add MC.example.com my_reg_key
```

However, if the device and the Firepower Management Center are separated by a NAT device, enter a unique NAT ID along with the registration key, and specify `DONTRESOLVE` instead of the hostname, for example:

```
configure manager add DONTRESOLVE my_reg_key my_nat_id
```

Procdure:

1. Log in to the device as a user with Configuration CLI access level:
   - If you are performing the initial setup from the console, you are already logged in as the `admin` user, which has the required access level.
   - Otherwise, SSH to the device's management IP address or host name.
2. At the prompt, register the device to a Firepower Management Center using the `configure manager add` command, which has the following syntax:

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

   where:

   `{hostname | IPv4_address | IPv6_address | DONTRESOLVE}` specifies either the fully qualified host name or IP address of the Firepower Management Center. If the Firepower Management Center is not directly addressable, use `DONTRESOLVE`.

   `reg_key` is the unique alphanumeric registration key, up to 37 characters in length, required to register a device to the Firepower Management Center.

   `nat_id` is an optional alphanumeric string used during the registration process between the Firepower Management Center and the device. It is required if the hostname is set to `DONTRESOLVE`.
3. Log out of the device.

   The device is ready to be added to a Firepower Management Center.

Next Steps

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*.

Note: If you want to use a serial or LOM/SOL connection to access your appliance's console, you should redirect console output; see Testing an Inline Bypass Interface Installation in the *Firepower Management Center Configuration Guide*. If you want to use LOM specifically, you must enable the feature as well as enable at least one LOM user; see Enabling LOM and LOM Users, page 32.

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.

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 Firepower 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.

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 Firepower Management Center to apply the same system policy to itself and all the devices it manages.

By default, the Firepower 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 Firepower 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.

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, Firepower devices 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. Note that while all Firepower devices support LOM, 7000 Series devices do not support LOM and physical serial access at same time. However, the console setting is the same regardless of which access method you want to use.

Using the Shell

You can use the shell to redirect the console output.

To redirect the console output using the shell:

1. Using your keyboard/monitor or serial connection, log into the appliance's shell using an account with Administrator privileges. The password is the same as the password for the appliance's web interface.
2. Type `expert` to display the shell prompt.

   The prompt for the appliance appears.
3. 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
     ```
4. To implement your changes, reboot the appliance by typing `sudo reboot`.

   The appliance reboots.

Using the Web Interface

You can also redirect console output through the web interface.

To redirect the console output using the web interface:

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 Firepower 7050 device.
   - The LOM settings appear.
   - Select **Lights-Out Management** to use LOM/SOL on a 7000 Series device (except the Firepower 7050).

   On these devices, you cannot use SOL and a regular serial connection at the same time. 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 32.

Restoring a Device 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

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

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 19.

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 31.

Before You Begin

- Obtain the restore ISO image for the appliance from the Support Site. See Obtaining the Restore ISO and Update Files, page 20.

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 21.

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.

   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.

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 22 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 23 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

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 23.

To start the restore utility:

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.

2. Reboot the appliance. On a Firepower device, type:

   ```
   system reboot
   ```

   The appliance reboots.

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:

     ```
     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 connection, type **Restore_Serial** at the prompt and press Enter.

   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 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

- Continue with Using the Interactive Menu to Restore an Appliance, page 24.

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 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 (eth0) management interface only.

Note: Before you can restore an appliance using LOM, you must enable the feature; see Setting Up Lights-Out Management, page 31.

To start the restore utility using Lights-Out Management:

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.

2. Reboot the appliance as root user. For a Firepower device, type:

   ```
   system reboot
   ```

   The appliance reboots.

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:

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

4. 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
   ```

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.

6. Press Enter to confirm the copyright notice.

What to Do Next

- Continue with Using the Interactive Menu to Restore an Appliance, page 24.

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 19.

The menu displays the options listed in the following table.

Table 2 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 25
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 26
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 27
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 27
5 Run the Install	Invoke the restore process.	Invoking the Restore Process, page 28
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 29
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 33

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 27. 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 29. After you load the configuration, skip to menu option **4**: Downloading the ISO and Update Files and Mounting the Image, page 27.

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

1. **1 IP Configuration** — see Identifying the Appliance's Management Interface, page 25.
2. **2 Choose the transport protocol** — see Specifying ISO Image Location and Transport Method, page 26.
3. **3 Select Patches/Rule Updates** (optional) — Updating System Software and Intrusion Rules During Restore, page 27.
4. **4 Download and Mount ISO** — see Downloading the ISO and Update Files and Mounting the Image, page 27.
5. **5 Run the Install** — see Invoking the Restore Process, page 28.

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 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 20), 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 3 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 **Note:** 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 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 main menu, select **2 Choose the transport protocol**.
2. On the page that appears, select either **HTTP**, **FTP**, or **SCP**.

   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.
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 3.

   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 27. 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 20.

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 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 26) 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 29.

To download and mount the ISO image:

1. From the 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 29.

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

1. From the 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 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 24.

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. From the main menu, select **5 Run the Install**.
2. Confirm that you want to restore the appliance and continue with the next 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 30.

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.

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.

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 19.

What to Do Next

- Continue with Next Steps, page 30.

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 25
- 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 26
- 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 27

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's 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 27.

To load a saved restore configuration:

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.
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 27.

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 19.

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 Using the Web Interface, page 12.
- 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 Installing the Firepower 7000 Series Device, page 9.

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" in the *Firepower 8000 Series Hardware Installation Guide*.

- 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 32.

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.

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.

Table 4 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.
-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: 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.

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 32
- Installing an IPMI Utility, page 33

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.
- 7000 Series devices can have up to eight 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. 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:

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/
```

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 24.

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 22
   - Starting the Restore Utility Using Lights-Out Management, page 23
2. From the 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 series documentation and where to find it, see the documentation roadmap at the following URL:

http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html