Cisco Secure Firewall Management Center 1700, 2700, and 4700 Getting Started Guide

First Published: 2023-11-28

Last Modified: 2023-11-28

About the Secure Firewall Management Center 1700, 2700, and 4700

The management center provides centralized, integrated, and streamlined management of threat defense devices. It also provides application control, intrusion prevention system (IPS), URL filtering, and malware protection functions. In a typical deployment on a large network, you install multiple managed threat defense devices on network segments. Each device controls, inspects, monitors, and analyzes traffic, and then reports to a management center.

The Secure Firewall Management Center 1700, 2700, and 4700 appliances provide significant performance and efficiency.

This doc explains how to complete the cabling and the initial configuration of the management center.

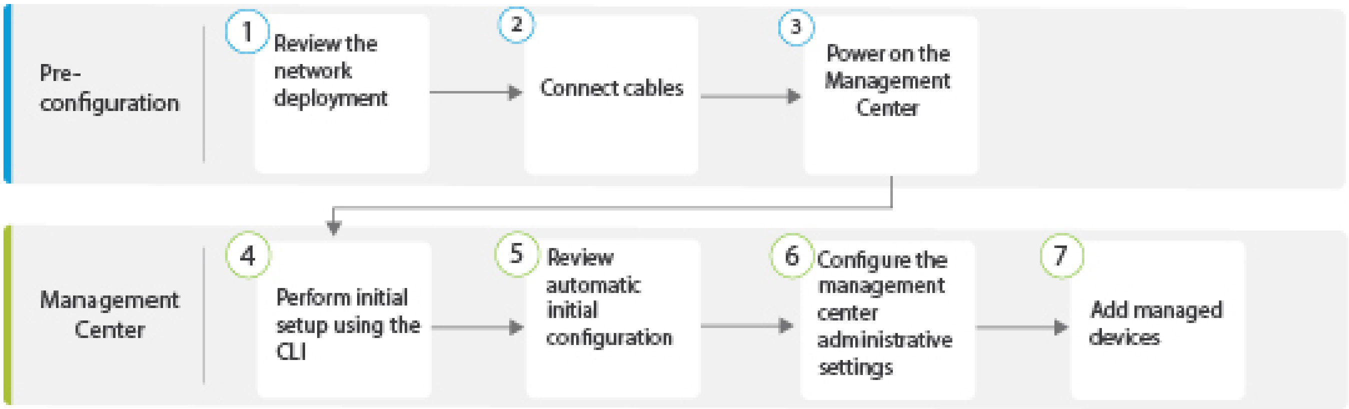
Before You Begin

Install the management center. For more information, see the *Cisco Secure Firewall Management Center 1700, 2700 and 4700 Hardware Installation Guide*.

For a complete list of the Cisco Secure Firewall series documentation and where to find it, see the documentation roadmap.

End-to-End Procedure

The following flowchart illustrates the tasks to deploy and configure the management center.

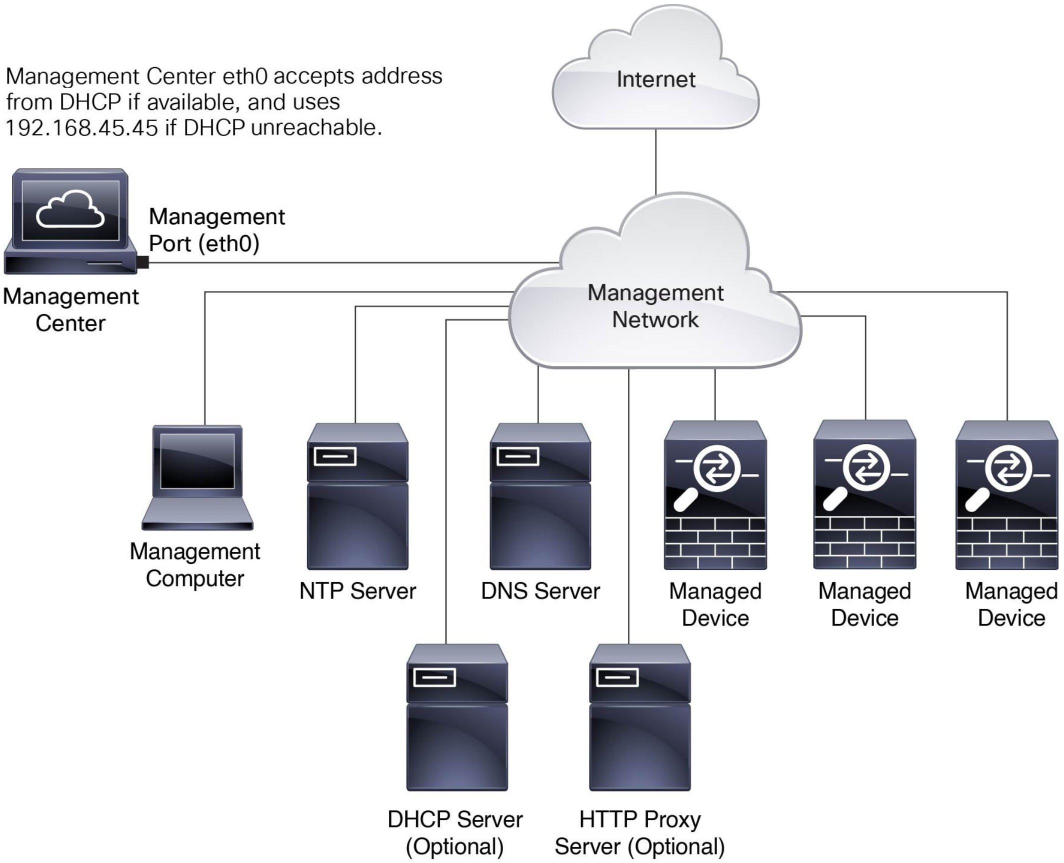

Pre-configuration
1 Review the network deployment
2 Connect cables
3 Power on the Management Center
Management Center
4 Perform initial setup using the CLI
5 Review automatic initial configuration
6 Configure the management center administrative settings
7 Add managed devices

①	Pre-Configuration	Review Network Deployment, on page 2
②	Pre-Configuration	Cable the Management Center, on page 4
③	Pre-Configuration	Power on the Management Center, on page 6
④	Management Center	Perform Initial Setup of the Management Center Using the CLI, on page 8
⑤	Management Center	Review Automatic Initial Configuration, on page 14
⑥	Management Center	Configure Management Center Administrative Settings, on page 15
⑦	Management Center	Add Managed Devices to the Management Center, on page 16

Review Network Deployment

Before you deploy the management center, you need information about the environment in which it operates.

The following figure shows a typical network deployment for a management center.



By default, the management center connects to your local management network through its management interface (eth0). This connection the management center communicates with a management computer, managed devices, services such as DHCP, DNS, NTP, and the internet.

The management center requires internet access to support Smart Licensing, Secure Firewall threat intelligence director, and malware defense services. Depending on the services provided by your local management network, the management center may also require internet access to reach an NTP or DNS server. You can configure your network to provide internet access to the management center directly or through a firewall device.

You can upload updates for system software, Vulnerability Database (VDB), Geolocation Database (GeoDB), and intrusion rules directly to the management center from an internet connection or from a local computer that has these updates from the internet.

To establish the connection between the management center and one of its managed devices, you need the IP address of at least one of the devices: the management center or the managed device. We recommend using both IP addresses if available. However, you may only know one IP address. For example, managed devices may be using private addresses behind NAT, so you only know the management center address. In this case, you can specify the management center address on the managed device plus a one-time, unique password of your choice called a NAT ID. On the management center, you specify the same NAT ID to identify the managed device.

The initial setup and configuration described in this document is for a management center that has internet access. If you deploy a management center in an air-gapped environment, see the Cisco Secure Firewall Management Center Administration Guide for your version for alternative methods you can use to support certain features such as configuring a proxy for HTTP communications, or using a Smart Software Satellite Server for Smart Licensing.

Initial Network Configuration for Management Centers

- Management Interface

  By default, the management center seeks out a local DHCP server for the IP address, network mask, and default gateway to use for the management interface (eth0). If the management center cannot reach a DHCP server, it uses the default IPv4 address 192.168.45.45, netmask 255.255.255.0, and gateway 192.168.45.1. During the initial setup, you can accept these defaults or specify different values.

  Note If you use DHCP, you must use DHCP reservation, so the assigned address does not change. If the DHCP address changes, device registration will fail because the management center network configuration gets out of sync. To recover from a DHCP address change, connect to the management center (using the hostname or the new IP address) and navigate to **System** (⚙) > **Configuration** > **Management Interfaces** to reset the network.

  If you use IPv6 addressing for the management interface, you must configure the address using the web interface after completing the initial setup.

- DNS Servers

  Specify IP addresses for up to two DNS servers. If you use an evaluation license, you may choose not to use DNS.

  Note During initial configuration, you can also provide a hostname and domain to facilitate communication between the management center and other hosts through DNS; you can configure more domains after completing the initial setup.

- NTP Servers

  Synchronize the system time on your management center and its managed devices during initial configuration. You can accept the default (0.sourcefire.pool.ntp.org and 1.sourcefire.pool.ntp.org as the primary and secondary NTP servers, respectively), or supply FQDNs or IP addresses for one or two trusted NTP servers reachable from your network. If you do not use DNS, you cannot use FQDNs to specify the NTP servers.

Cable the Management Center

You can cable the management center using one or more of the three connections listed below:

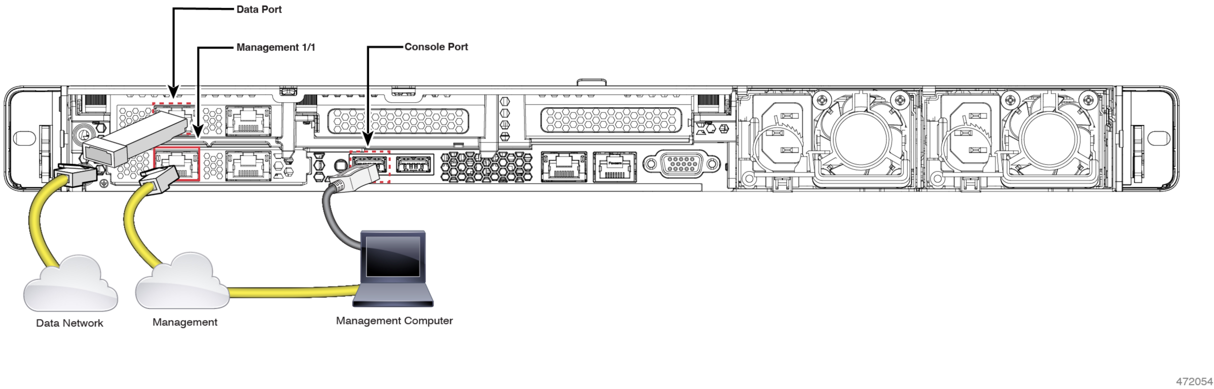
- Connect a keyboard to the USB port and a monitor to the VGA port of the management center. By default, the management center sends console messages to the VGA port.
- Connect the management center **CIMC** port to a local network reachable from a local computer where you can run an IPMI utility for Lights-Out Management. To use this connection see Set Up Light-Out Management, on page 17.

- Connect a local computer to the management center serial port as described in the procedure below.

AC power supplies have internal grounding so no additional chassis grounding is required when the supported AC power cords are used. For more information about supported power cords, see the *Cisco Secure Firewall Management Center 1700, 2700 and 4700 Hardware Installation Guide*

After rack-mounting the chassis, follow these steps to connect the cables.

Figure 1: Cable the Appliance to a Management Network



Before you begin

Important Read the Regulatory and Compliance Safety Information document before installing the management center chassis.

Rack-mount the appliance as described in the *Cisco Secure Firewall Management Center 1700, 2700, and 4700 Hardware Installation Guide.*

If you plan to cable the appliance using the console port and a local computer, redirect the console output to the console port. For more information, see Redirect the Console Output Using the Web Interface, on page 11 and Redirect the Console Output Using the CLI, on page 11.

Procedure

Step 1 Cable the following to your management network:

- Management 1/1 interface
- Management computer

Step 2 Connect the management computer to the console port using an RJ-45 to DB-9 console cable. Use the console port to access the CLI for initial setup.

Step 3 Use a terminal emulation software (such as HyperTerminal or XModem) on the local computer to interact with the management center. Set the terminal emulator for 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control.

Step 4 (Optional) Install any supported SFP+ transceiver and cable in the 10-Gigabit Ethernet SFP+ interface (data port) for management center 1700, 2700, and 4700, or the 25-Gigabit Ethernet SFP+ interface for management center 4700. Connect this interface to the same or different network from your other management interfaces depending on your network needs.

Note We recommend that you use only the supported SFP+ transceivers. For more information about the SFPs that 1700, 2700, and 4700 support, see the *Cisco Secure Firewall Management Center 1700, 2700 and 4700 Hardware Installation Guide*.

What to do next

1. Power on the Management Center, on page 6
2. Perform Initial Setup of the Management Center Using the CLI, on page 8

Power on the Management Center

The management center 1700, 2700, and 4700 appliances use 1050-W AC power supplies. For more information about the power supplies and the supported power cords, see the *Cisco Firepower Management Center 1700, 2700, and 4700 Hardware Installation Guide.*

Before you begin

It is important that you provide reliable power for your device, for example, use an uninterruptable power supply (UPS). Loss of power without first shutting down the chassis can cause serious file system damage.

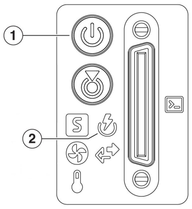
Procedure

Step 1 Use one of the supported power cords to connect the power supplies of the chassis to your power source.

Note We recommend connecting both power supplies on the management center. The appliance generates a health alert if only one power supply is connected.

Step 2 Press the Power button (labeled "**1**") on the front of the chassis, and verify that the power supply status LED (labeled "**2**") is on.

Figure 2: Power Button and Power Supply Status LED



Access the CLI or the Linux Shell on the Management Center

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

Before you begin

Establish a direct physical connection with the management center using the serial port, a keyboard and monitor, or establish an SSH session with the management center interface.

Procedure

Step 1 Log in to the management center using the credentials for the CLI **admin** user.

This action gives you access to the management center CLI.

Step 2 Use the **show version** command to verify the management center software version.

Example:

```
> show version
-----------[ firepower ]------------
Model                   : Cisco Firewall Management Center 4700 (66) Version 7.4.0 (Build
1482)
UUID                    : a10ed34e-d127-11e8-b440-728439d95305
Rules update version    : 2023-11-15-001-vrt
LSP version             : lsp-rel-20231115-1600
VDB version             : 375
----------------------------------------------------
```

Step 3 To access the Linux shell from the management center CLI, enter the **expert** command.

Shutdown or Restart the Management Center

Use the web interface to initiate an orderly shutdown or restart.

You can also shut down the management center using the **system shutdown** command from the management center CLI.

Tip For virtual devices, see the documentation for your virtual platform. For VMware in particular, custom power options are part of VMware Tools.

Caution Do not shutdown the management center using the power button; this action can cause data loss. Using the web interface or the **shutdown** command prepares the system to safely power off and restart without losing configuration data.

Procedure

Step 1 Log in to your management center, choose **System** (⚙) > **Configuration** > **Process**.

Step 2 Choose one of the following:

- **Shutdown Management Center** to initiate a graceful shutdown of the management center.
- **Reboot Management Center** to shut down and restart the management center gracefully.
- **Restart Management Center Console** to restart the communications, database, and HTTP server processes. This action is typically used during troubleshooting, and may cause deleted hosts to reappear in the network map.

Perform Initial Setup of the Management Center Using the CLI

You can also perform the initial setup using the CLI. You must complete an Initial Configuration Wizard that configures the new appliance to communicate on your trusted management network.

Before you begin

- Cable the management center as described in Cable the Management Center, on page 4.
- Ensure that you have the following information for the management center to communicate on your management network:
  - An IPv4 management IP address
  - A network mask and a default gateway (if not using DHCP)
- Connect to the management center using one of three methods:

- Connect a USB keyboard and VGA monitor to the management center for console access.
- Connect a local computer to the management center serial port with an RJ-45 to DP-9 console cable.
- After configuring the IP using the above two methods, access the device using SSH to connect to the management center using the IPv4 management IP address.

Procedure

Step 1 Log in to the management center at the console using **admin** as the username and **Admin123** as the password for the **admin** account. The password is case-sensitive.

Step 2 When prompted, press **Enter** to display the End User License Agreement (EULA).

Step 3 Review the EULA. When prompted, enter **`yes`**, **`YES`**, or press **Enter** to accept the EULA.

Important You cannot proceed without accepting the EULA. If you respond with anything other than **`yes`**, **`YES`**, or **Enter**, the system logs you out.

Step 4 To ensure system security and privacy, the first time you log in to the management center you are required to change the **admin** password. When the system prompts for a new password, enter a new password complying with the restrictions, and enter the same password again when the system prompts for confirmation.

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

Note On completion of the initial configuration process, the system sets the passwords for the two **admin** accounts (one for web access and the other for CLI access) to the same value, complying with the strong password requirements described in the Cisco Secure Firewall Management Center Administration Guide. If you change the password for either **admin** account thereafter, they are no longer be the same. You can remove the strong password requirement from the web interface **admin** account.

Step 5 Configure the network settings.

When you follow the prompts, your options appear in parentheses such as **`(y/n)`**. Defaults are listed in square brackets such as **`[y]`**. Note the following when responding to the prompts:

- If you are setting up an appliance after restoring it to factory defaults and you did not delete the appliance's license and network settings, the prompts are prepopulated with the retained values.
- Press **Enter** to accept the default.
- For hostname, enter a fully qualified domain name (`<hostname>.<domain>`) or host name. This field is required.
- If you use DHCP, you must use DHCP reservation, so the assigned address does not change. If the DHCP address changes, device registration will fail because the management center network configuration gets out of sync. To recover from a DHCP address change, connect to the management center (using the hostname or the new IP address) and navigate to **System** (⚙) > **Configuration** > **Management Interfaces** to reset the network.

- If you choose to configure IPv4 manually, the system prompts for the IPv4 address, netmask, and default gateway.
- Configuring a DNS server is optional; to specify no DNS server enter **`none`**. Otherwise specify IPv4 addresses for one or two DNS servers. If you specify two addresses, separate them with a comma. If you specify more than two DNS servers, the system ignores the additional entries. If your management center does not have internet access, you cannot use a DNS outside of your local network.

  Note If you use an evaluation license, specifying DNS is optional, but DNS is required to use permanent licenses for your deployment.

- You must enter the fully qualified domain name or IP address for at least one NTP server reachable from your network. You may not specify FQDNs for NTP servers if you are not using DHCP. You may specify two servers (a primary and a secondary); separate their information with a comma. If you specify more than two DNS servers, the system ignores the additional entries. If your management center does not have internet access, you cannot use an NTP server outside of your local network.

Example:

```
Enter a hostname or fully qualified domain name for this system [firepower]: fmc
Configure IPv4 via DHCP or manually? (dhcp/manual) [DHCP]: manual
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.0.66
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.224
Enter the IPv4 default gateway for the management interface [ ]: 10.10.0.65
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
208.67.222.222,208.67.220.220
Enter a comma-separated list of NTP servers [0.sourcefire.pool.ntp.org,
1.sourcefire.pool.ntp.org]:
```

Step 6 Review the settings. The system displays a summary of the configurations.

Example:

```
Hostname:                            fmc
IPv4 configured via:                 manual configuration
Management interface IPv4 address:   10.10.0.66
Management interface IPv4 netmask:   255.255.255.224
Management interface IPv4 gateway:   10.10.0.65
DNS servers:                         208.67.222.222,208.67.220.220
NTP servers:                         0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org
```

Step 7 Confirm the settings.

- If the settings are correct, enter **`y`** and press **Enter** to accept the settings and continue.
- If the settings are incorrect, enter **`n`** and press **Enter**. The system prompts for the information again, beginning with the hostname.

Example:

```
Are these settings correct? (y/n) y
If your networking information has changed, you will need to reconnect.

Updated network configuration.
```

Step 8 After you accept the settings, you can enter **`exit`** to exit the management center CLI.

What to do next

- Connect to the management center web interface using the network information that you have configured.
- Review the weekly maintenance activities that the management center configures automatically as part of the initial configuration process. These activities are designed to keep your system up to date and your data backed up. For more information, see Review Automatic Initial Configuration, on page 14 .
- Configure the management center for IPv6 addressing after completing the initial setup using the web interface, if required. For more information, see Cisco Secure Firewall Management Center Device Configuration Guide.
- (Optional) Configure the management center for SOL or LOM access as described in Set Up Light-Out Management, on page 17.

Redirect the Console Output Using the Web Interface

You must be an Admin user to perform this procedure.

Before you begin

- Complete the initial setup process of the appliance.
- Disable Spanning Tree Protocol (STP) on any third-party switching equipment connected to the device's management interface.

Procedure

Step 1 Choose **System** (⚙) > **Configuration**.

Step 2 Choose **Console Configuration**.

Step 3 Select a remote console access option:

- (Default) Choose **VGA** to use the appliance’s VGA port.
- Choose **Physical Serial Port** to use the appliance’s serial port.

Step 4 Click **Save**.

Redirect the Console Output Using the CLI

Before you begin

Complete the initial setup process of the management center.

Procedure

Step 1 Use the management center CLI **admin** credentials to access the Linux shell on the management center. For more information, see Access the CLI or the Linux Shell on the Management Center, on page 7.

Step 2 At the prompt, use one of the following commands to set the console output:

- To direct console messages to the VGA port: `sudo /usr/local/sf/bin/configure_console.sh vga`
- To direct console messages to the physical serial port: `sudo /usr/local/sf/bin/configure_console.sh serial`

Step 3 To implement your changes, reboot the appliance by using the `sudo reboot` command.

Reset the CLI Admin Password

You can change the password for the admin account to access the management center CLI.

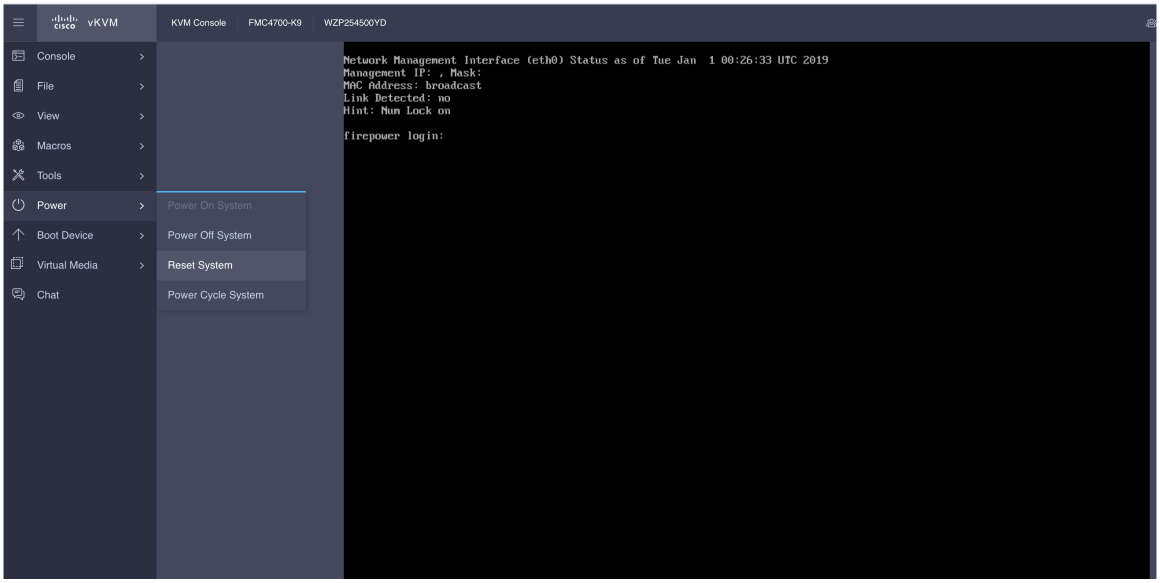
Before you begin

To reset the admin password, you must establish a console connection with the appliance.

Procedure

Step 1 Log in to the management center CLI as the admin user.

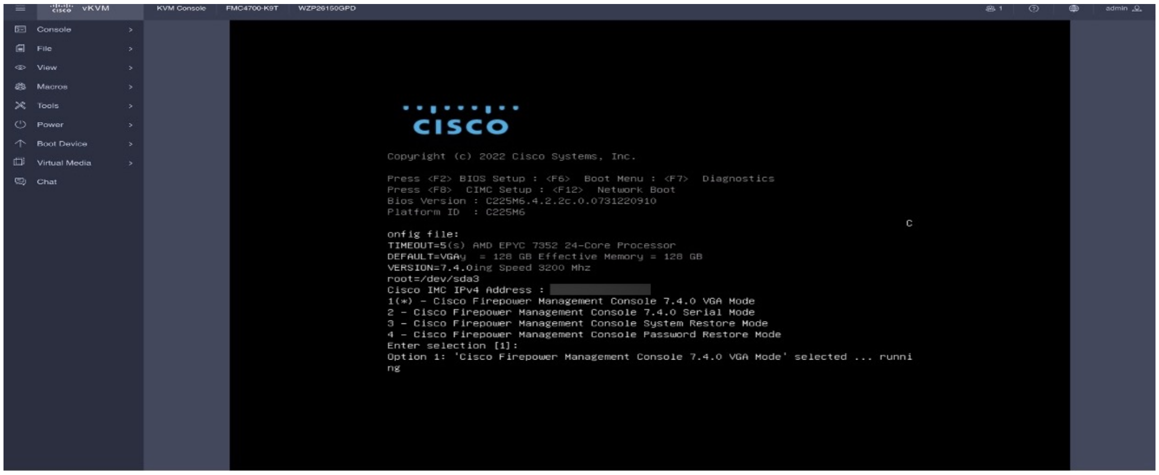
Step 2 In the console, choose **Power** > **Reset System**.



```
Network Management Interface (eth0) Status as of Tue Jan  1 00:26:33 UTC 2019
Management IP: , Mask:
MAC Address: broadcast
Link Detected: no
Hint: Num Lock on

firepower login:
```

The following messages appear in the console:

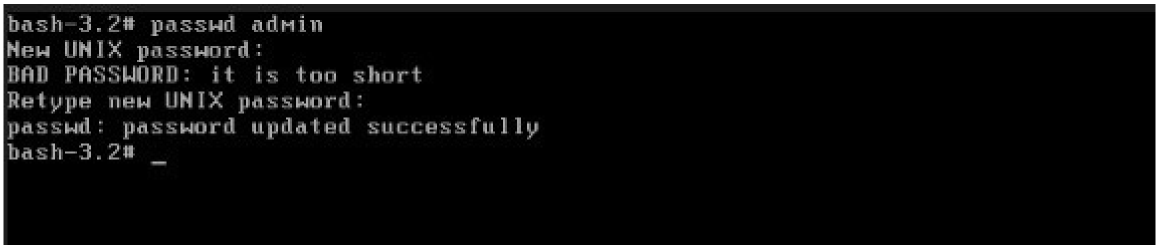


```
Copyright (c) 2022 Cisco Systems, Inc.

Press <F2> BIOS Setup : <F6>  Boot Menu : <F7>  Diagnostics
Press <F8>  CIMC Setup : <F12>  Network Boot
Bios Version : C225M6.4.2.2c.0.0731220910
Platform ID  : C225M6
                                                                    C
onfig file:
TIMEOUT=5(s) AMD EPYC 7352 24-Core Processor
DEFAULT=VGAy  = 128 GB Effective Memory = 128 GB
VERSION=7.4.0ing Speed 3200 Mhz
root=/dev/sda3
Cisco IMC IPv4 Address : [redacted]
1(*) - Cisco Firepower Management Console 7.4.0 VGA Mode
2 - Cisco Firepower Management Console 7.4.0 Serial Mode
3 - Cisco Firepower Management Console System Restore Mode
4 - Cisco Firepower Management Console Password Restore Mode
Enter selection [1]:
Option 1: 'Cisco Firepower Management Console 7.4.0 VGA Mode' selected ... runni
ng
```

Step 3 Enter option 4 to reset the password.

Step 4 At the # prompt, enter the **passwd admin** command.



```
bash-3.2# passwd admin
New UNIX password:
BAD PASSWORD: it is too short
Retype new UNIX password:
passwd: password updated successfully
bash-3.2# _
```

Step 5 Enter the new admin password.

Note We recommend that you use a complex password.

Step 6 Enter the **reboot** command. Allow the reboot process to complete.

Reset the Web Interface Admin Password

You can change the password for the admin account to access the management center web interface.

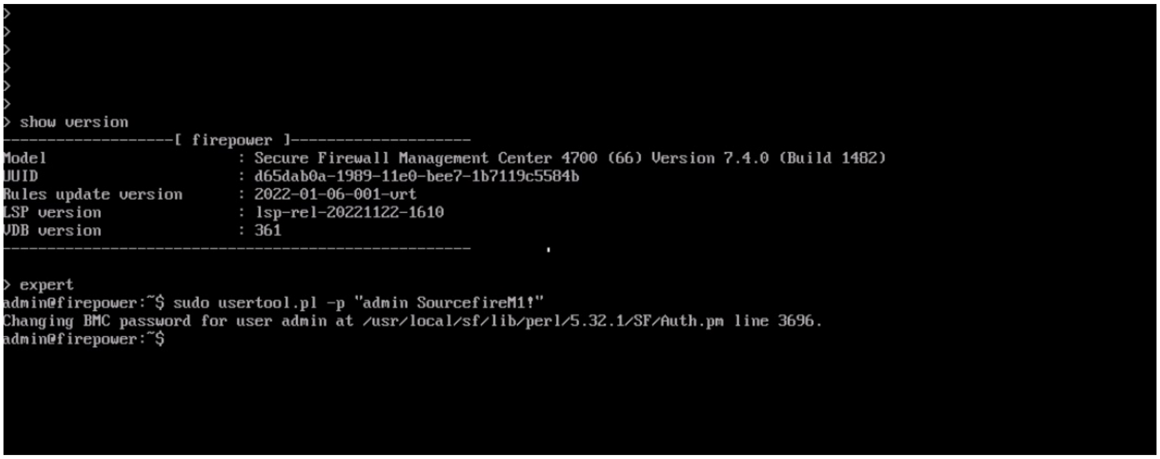
Procedure

Step 1 Log in to the web interface for the management center as the admin user. To reset the admin password, you need to establish a console connection with the appliance.

Step 2 To access the Linux shell, enter the **expert** command.

Step 3 At the shell prompt, enter the **sudo usertool.pl -p "admin password"** command. Here *password* is the new password for the web interface admin user.

In the following example, the password is **SourcefireM1!**.



```
>
>
>
>
>
>
> show version
-------------------[ firepower ]--------------------
Model                     : Secure Firewall Management Center 4700 (66) Version 7.4.0 (Build 1482)
UUID                      : d65dab0a-1989-11e0-bee7-1b7119c5584b
Rules update version      : 2022-01-06-001-vrt
LSP version               : lsp-rel-20221122-1610
VDB version               : 361
----------------------------------------------------

> expert
admin@firepower:~$ sudo usertool.pl -p "admin SourcefireM1!"
Changing BMC password for user admin at /usr/local/sf/lib/perl/5.32.1/SF/Auth.pm line 3696.
admin@firepower:~$
```

Step 4 At the password prompt, enter the new password.

Review Automatic Initial Configuration

As part of the initial configuration, the management center automatically configures maintenance tasks to keep your system up-to-date and your data backed up.

These tasks are scheduled in UTC, which means that when they occur *locally* depends on the date and your specific location. As the tasks are scheduled in UTC, they do not adjust for daylight saving time, summer time, or any such seasonal adjustments that you may observe in your location. If you are affected, scheduled tasks occur one hour later in the summer than in the winter, according to local time.

Note We *strongly* recommend you review the auto-scheduled configurations, confirm that the management center has established them successfully, and adjust them if necessary.

Table 1: Maintenance Tasks for Your Management Center

Task	Description	GUI Path	More Info
Weekly GeoDB updates	GeoDB is a database to view and filter traffic based on the geographical location.	**System** > **Updates** > **Geolocation Updates** > **Recurring Geolocation Updates**	*Cisco Secure Firewall Management Center Administration Guide*
Weekly management center software updates	The management center automatically schedules a weekly task to download the latest software for the management center and its managed devices.	**System** > **Tools** > **Scheduling**	

Task	Description	GUI Path	More Info
Weekly management center configuration backup	The management center automatically schedules a weekly task to perform a locally stored configuration-only backup.	**System** > **Tools** > **Scheduling**	*Cisco Secure Firewall Management Center Administration Guide*
Vulnerability database update	The management center downloads and installs the latest vulnerability database (VDB) update from the Cisco support site. This is a one-time operation.	**System** > **Tools** > **Scheduling**	*Cisco Secure Firewall Management Center Administration Guide*
Daily intrusion rule update	The management center configures a daily automatic intrusion rule update from the Cisco support site. The management center deploys automatic intrusion rule updates to the affected managed devices when it next deploys affected policies.	**System** > **Updates** > **Rule Updates**	

Configure Management Center Administrative Settings

After you complete the initial setup for the management center and verify its success, we recommend that you complete some administrative tasks for your deployment. You must complete any tasks that you skipped during the initial setup, such as licensing. Establish these configurations using the default **admin** account or another account with Administrator access.

In a NAT environment where multiple management centers share the same IP address and are differentiated by port numbers. Note the following conditions:

- Each management center can support only one login session at a time.
- To access different management centers, use a different browser for each login (for example Firefox and Chrome), or set the browser to incognito or private mode.

Procedure

Step 1 Log in to your management center.

Step 2 In the **Username** and **Password** fields, enter your username and password.

Step 3 Click **Login**.

Step 4 Configure the following administrative tasks:

Task	GUI Path	More Info
Create user account	**System** > **Users**	*Cisco Secure Firewall Management Center Administration Guide*
Configure time settings	**System** > **Configuration** > **Time Synchronization**	
Configure smart licensing	**System** > **Licenses** > **Smart Licenses**	

Add Managed Devices to the Management Center

For each managed device, use these instructions to establish a simple deployment that does not include multitenancy, clusters, or high availability. To configure a deployment using any of these features, see the Cisco Secure Firewall Management Center Device Configuration Guide for your version.

Before you begin

- Perform the device-specific setup activities and configure the device for remote management.

Important Note the registration key that you use for the device.

- If your environment uses NAT, note the NAT ID used during device setup.
- If your environment uses DNS, note the hostname that resolves to a valid IP address for the device. If your environment uses DHCP to assign IP addresses, use a host name to identify the device rather than an IP address.
- If your environment does not use DNS, you need the IP address for the device.
- Determine the licenses needed for the managed device and add them to the management center; you can add the licenses to the managed device during the process of adding it to the management center.
- Assign an access control policy to the managed device after you add it to the management center. The instructions below include a procedure to establish a basic access control policy for this purpose.

Procedure

Step 1 Choose **Devices** > **Device Management** > **Add** > **Add Device**.

Step 2 In the **Host** field, enter the IP address or the hostname of the device.

The hostname of the device is the fully qualified name or the name that resolves through the local DNS to a valid IP address. Use a hostname rather than an IP address if your network uses DHCP to assign IP addresses.

In a NAT environment, you do not need to specify the IP address or hostname of the device, if you already specified the IP address or hostname of the management center when you configured the device to be managed by the management center.

Step 3 In the **Display Name** field, enter a name for the device as you want it to appear in the management center web interface.

Step 4 In the **Registration Key** field, enter the same registration key that you used when you configured the device to be managed by the management center. This key is a one-time-use shared secret that you configured when you originally identified this management center on the device.

Step 5 Choose an initial **Access Control Policy**. Unless you have a customized policy, choose **Create new policy**, and choose **Block all traffic**. You can change this later to allow traffic.

If the device is incompatible with the policy you choose, the deployment fails. This incompatibility can occur for multiple reasons, including licensing mismatches, model restrictions, passive and inline issues, and other misconfigurations. For more information, see the Cisco Secure Firewall Management Center Device Configuration Guide. After you resolve the issue, manually deploy configurations to the device.

Step 6 Choose licenses to apply to the device.

Step 7 If you used a NAT ID during device setup, expand the **Advanced** section and enter the same NAT ID in the **Unique NAT ID** field.

Step 8 Click **Register**.

It may take up to two minutes for the management center to verify the device's heartbeat and establish communication.

Set Up Light-Out Management

The LOM feature allows you to perform a limited set of actions on the management center using a Serial over LAN (SOL) connection. With LOM, you use a CLI 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.

Note You can use LOM only on the CIMC interface.

If you need to restore the management center to factory defaults and do not have physical access to the appliance, you can use LOM to perform the restore process.

Caution The restore process resets the LOM settings on the device; you cannot access a newly restored appliance using LOM. When restoring a device to factory settings using LOM, if you do not have physical access to the appliance and you delete the license and network settings, you cannot access the appliance after the restore.

Note Firewall appliances also support LOM. You can configure LOM and LOM users for each appliance using each appliance's local web interface. You cannot use the management center to configure LOM on a firewall device. Similarly, because users are managed independently for each appliance, enabling or creating an LOM-enabled user on the management center does not transfer that capability to users on firewall devices.

Prerequisites

- Install an Intelligent Platform Management Interface (IMPI) utility on your local computer. For more information, see IPMI Utility Installation, on page 18.
- Determine which commands are needed to access an appliance using the IPMI tool. For more information, see Cisco Secure Firewall Management Center Administration Guide.

To setup LOM:

Step	Task	GUI Path	More Info
1	Enable LOM	**System** > **Users** > **Users**	Cisco Secure Firewall Management Center Administration Guide
2	Enable LOM user access	**System** > **Configuration** > **Console Configuration** > **Lights-Out Management**	Cisco Secure Firewall Management Center Administration Guide
3	Use a third-party IPMI utility to create a SOL connection to the appliance.	-	IPMI Utility Installation, on page 18

IPMI Utility Installation

You can use a third-party IPMI utility on your computer to create an SOL connection to the appliance. IPMItool is standard with many Linux distributions, but on Mac and Windows systems you must install a utility.

If your computer is running Mac OS, install IPMItool. First, confirm that your Mac has Apple's Xcode developer tools package installed. Ensure that 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, see https://developer.apple.com/technologies/tools/ and 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, see http://ipmiutil.sourceforge.net/.

Preconfigure Management Centers

You can preconfigure your management center at a staging location (a central location to preconfigure or stage multiple appliances) and deploy it at a target location (any location other than the staging location).

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

1. Install the system on the device at the staging location.
2. Shut down and ship the appliance to the target location.
3. Deploy the appliance at the target location.

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

Prerequisites for Preconfiguration

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

During the initial setup, you configure your appliance with enough information to connect the appliance to the network and install the system.

You need the following information to preconfigure your appliance:

- New password (initial setup requires changing the password)
- Hostname of the appliance
- Domain name of the appliance
- IP management address of the appliance
- Network mask of the appliance at the target location
- Default gateway of the appliance at the target location
- IP address of the DNS server at the staging location, or, if accessible, the target location
- IP address of the NTP server at the staging location, or, if accessible, the target location

Optional Preconfiguration Information

You can change some default configurations, including the following:

- The time zone (if you choose to manually set the time for your appliances)
- The remote storage location for automatic backups
- The LOM IP address to enable LOM

Preconfigure Time Management

Procedure

Step 1 Synchronize time to a physical NTP server.

Step 2 Set the IP addresses for the DNS and NTP servers using one of the following methods:

- If your network at the staging location can access the DNS and NTP servers at the target location, use the IP addresses for the DNS and NTP servers at the target location.
- If your network at the staging location cannot access the DNS and NTP servers at the target location, use the staging location information and reset the appliance at the target location.

Step 3 Use the time zone for the target deployment if you set the time on the appliance manually instead of using NTP. For more information, see the Cisco Secure Firewall Management Center Administration Guide for your version.

Prepare the Management Center for Shipment

Procedure

Step 1 Install the chassis according to the instructions in the *Cisco Secure Firewall Management Center 1700, 2700, and 4700 Hardware Installation Guide*.

Step 2 Cable the appliance and power on the appliance.

Step 3 Perform initial setup of the appliance using the CLI.

Step 4 Safely power down the management center.

Step 5 Ensure that your appliance is safely prepared for shipping. For more information, see Shipping Considerations, on page 20.

Shipping Considerations

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

- Use the original packaging to repack the appliance.
- Include all reference material and power cords with the appliance.
- Provide all setting and configuration information to the target location, including the new password and the detection mode.

Troubleshooting the Appliance Preconfiguration

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

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

- Confirm that all power cables and communication cables are connected properly to the appliance.
- Confirm that you have the current password for your appliance. The initial setup at the staging location prompts you to change your password. See the configuration information provided by the staging location for the new password.

- Confirm that the network settings are correct. For more information, see Perform Initial Setup of the Management Center Using the CLI, on page 8.
- Confirm that the correct communication ports are functioning properly. For information about managing firewall ports and the required open ports, see the Cisco Secure Firewall Management Center Administration Guide for your version.

If you continue to experience difficulty logging in to the appliance, contact Cisco TAC.

Power Off the Management Center

It is important that you shut down your system properly. Simply unplugging the power or pressing the power switch can cause serious file system damage. There are many background processes running all the time, and unplugging or shutting off the power does not allow the graceful shutdown of your appliance.

You can power off the device by using one of the following methods:

- The web interface of the management center device management page. Choose **System** > **Configuration** > **Process** > **Shutdown Management Center**.
- The **shutdown** command from management center CLI.

For virtual devices, you can power off the host. For more information, see to the documentation for your virtual platform. For VMware in particular, custom power options are part of VMware Tools.

What's Next?

To continue configuring your management center, see the *Cisco Secure Firewall Management Center Administration Guide* and *Cisco Secure Firewall Management Center Configuration Guide*.