Firewall Management Center Virtual Initial Setup

This chapter describes the initial setup process you need to perform after you deploy the Firewall Management Center Virtual appliance.

Firewall Management Center Initial Setup Using the CLI for Versions 6.5 and Later

After you deploy an Firewall Management Center Virtual, you can access the appliance console for initial setup.You can perform initial setup using the CLI as an alternative to using the web interface. You must complete an Initial Configuration Wizard that configures the new appliance to communicate on your trusted management network. The wizard requires that you accept the end user license agreement (EULA) and change the administrator password.

Before you begin

- Be sure you have the following information needed for the Firewall Management Center Virtual to communicate on your management network:
  - An IPv4 management IP address.

    The Firewall Management Center interface is preconfigured to accept an IP4 address assigned by DHCP. Consult with your system administrator to determine what IP address your DHCP has been configured to assign to the Firewall Management Center MAC address. In scenarios where no DHCP is available, the Firewall Management Center interface uses the IPv4 address 192.168.45.45.
  - A network mask and a default gateway (if not using DHCP).

Procedure

Step 1 Log into the Firewall Management Center Virtual at the console using **admin** as the username and **Admin123** as the password for the **admin** account. Note that 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 Firewall 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 displayed, and enter the same password again when the system prompts for confirmation.

Note
The Firewall 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* for your version. If you change the password for either **admin** account thereafter, they will no longer be the same, and the strong password requirement can be removed from the web interface **admin** account.

Step 5 Answer the prompts to configure network settings.

When following the prompts, for multiple-choice questions, your options are listed in parentheses, such as **`(y/n)`**. Defaults are listed in square brackets, such as **`[y]`**. Note the following when responding to prompts:

- Press **Enter** to accept the default.
- For hostname, supply 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 Firewall Management Center network configuration gets out of sync. To recover from a DHCP address change, connect to the Firewall 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 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 Firewall Management Center does not have internet access you cannot use a DNS outside of your local network.

  Note
  If you are using an evaluation license, specifying DNS is optional at this time, 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 Firewall 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' [CiscoUmbrella]: 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 The system displays a summary of your configuration selections. Review the settings you have entered.

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 The final prompt gives you the opportunity to 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 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 have accepted the settings, you can enter **exit** to exit the Firewall Management Center CLI.

What to do next

- You can connect to the Firewall Management Center Virtual web interface using the network information you have just configured.
- Review the weekly maintenance activites the Firewall Management Center configures automatically as a part of the initial configuration process. These activities are designed to keep your system up-to-date and your data backed up. See Review Automatic Initial Configuration for Versions 6.5 and Later, on page 7 .
- You can configure the Firewall Management Center for IPv6 addressing after completing the initial setup using the web interface as described in the *Cisco Secure Firewall Management Center Device Configuration Guide* for your version.

Perform Initial Setup at the Web Interface for Versions 6.5 and Later

After you deploy a Firewall Management Center Virtual, you can perform initial setup using HTTPS at the appliance web interface.

When you log into the Firewall Management Center web interface for the first time, the Firewall Management Center presents an Initial Configuration Wizard to enable you to quickly and easily configure basic settings for the appliance. This wizard consists of three screens and one pop-up dialog box:

- The first screen forces you to change the password for the **admin** user from the default value of **Admin123**.
- The second screen presents the End User License Agreement (EULA), which you are required to accept before using the appliance.
- The third screen allows you to change network settings for the appliance management interface. This page is prepopulated with current settings, which you may change.
- The wizard performs validation on the values you enter on this screen to confirm the following:
  - Syntactical correctness
  - Compatibility of the entered values (for instance, compatible IP address and gateway, or DNS provided when NTP servers are specified using FQDNs)
  - Network connectivity between the Firewall Management Center Virtual and the DNS and NTP servers

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

  The system does not perform connectivity testing if you enter configuration values that would result in cutting off the existing connection between the Firewall Management Center Virtual and the browser. In this case the wizard displays no connectivity status information for DNS or NTP.
- After you have completed the three wizard screens, a pop-up dialog box appears that offers you the opportunity to (optionally) quickly and easily set up Smart Licensing.

When you have completed the Initial Configuration Wizard and completed or dismissed the Smart Licensing dialog, the system displays the device management page, described in “Device Management” in the *Cisco Secure Firewall Management Center Device Configuration Guide* for your version.

Before you begin

- Be sure you have the following information needed for the Firewall Management Center to communicate on your management network:
  - An IPv4 management IP address.

The Firewall Management Center interface is preconfigured to accept an IP4 address assigned by DHCP. Consult with your system administrator to determine what IP address your DHCP has been configured to assign to the Firewall Management Center MAC address. In scenarios where no DHCP is available, the Firewall Management Center interface uses the IPv4 address 192.168.45.45.

- A network mask and a default gateway (if not using DHCP).

- If you are not using DHCP, configure a local computer with the following network settings:
  - IP address: 192.168.45.2
  - Netmask: 255.255.255.0
  - Default gateway: 192.168.45.1

Disable any other network connections on this computer.

Procedure

Step 1 Use a web browser to navigate to the Firewall Management Center Virtual's IP address: *https://<Management Center-IP>*.

The login page appears.

Step 2 Log into the Firewall Management Center Virtual using **admin** as the username and **Admin123** as the password for the admin account. (The password is case-sensitive.)

Step 3 At the **Change Password** screen:

a) (Optional) Check the **Show password** check box to see the password while using this screen.

b) (Optional) Click the **Generate Password** button to have the system create a password for you that complies with the listed criteria. (Generated passwords are nonmnemonic; take careful note of the password if you choose this option.)

c) To set a password of your choosing, enter a new password in the **New Password** and **Confirm Password** text boxes.

The password must comply with the criteria listed in the dialog.

Note
The Firewall 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. The password must comply with the strong password requirements described in the *Cisco Secure Firewall Management Center Administration Guide* for your version. If you change the password for either **admin** account thereafter, they will no longer be the same, and the strong password requirement can be removed from the web interface **admin** account.

d) Click **Next**.

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

Step 4 At the **User Agreement** screen, read the EULA and click **Accept** to proceed.

If you click **Decline** the wizard logs you out of the Firewall Management Center Virtual.

Step 5 Click **Next**.

Step 6 At the **Change Network Settings** screen:

a) Enter a **Fully Qualified Domain Name**. If default value is shown, you may use that if it is compatible with your network configuration. Otherwise, enter a fully qualified domain name (syntax `<hostname>.<domain>`) or hostname.

b) Choose the boot protocol for the **Configure IPv4** option, either **Using DHCP** or **Using Static/Manual**.

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 Firewall Management Center network configuration gets out of sync. To recover from a DHCP address change, connect to the Firewall Management Center (using the hostname or the new IP address) and navigate to **System** > **Configuration** > **Management Interfaces** to reset the network.

c) Accept the displayed value, if one is shown, for **IPv4 Address** or enter a new value. Use dotted decimal form (for example, 192.168.45.45).

Note
If you change the IP address during initial configuration, you need to reconnect to the Firewall Management Center using the new network information.

d) Accept the displayed value, if one is shown, for **Network Mask** or enter a new value. Use dotted decimal form (for example, 255.255.0.0).

Note
If you change the network mask during initial configuration, you need to reconnect to the Firewall Management Center using the new network information.

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

Note
If you change the gateway address during initial configuration, you may need to reconnect to the Firewall Management Center using the new network information.

f) (Optional) For **DNS Group** you can accept the default value, **Cisco Umbrella DNS**.

To change the DNS settings, choose **Custom DNS Servers** from the drop-down list, and enter IPv4 addresses for the **Primary DNS** and **Secondary DNS**. If your Firewall Management Center does not have internet access you cannot use a DNS outside of your local network. Configure no DNS Server by choosing **Custom DNS Servers** from the drop-down list and leaving the **Primary DNS** and **Secondary DNS** fields blank.

Note
If you use FQDNs rather than IP addresses to specify NTP servers, you must specify DNS at this time. If you are using an evaluation license DNS is optional, but DNS is required to use permanent licenses for your deployment.

g) For **NTP Group Servers** you can accept the default value, **Default NTP Servers**. In this case the system uses **0.sourcefire.pool.ntp.org** as the primary NTP server, and **1.sourcefire.pool.ntp.org** as the secondary NTP server.

To configure other NTP servers, choose **Custom NTP Group Servers** from the drop-down list and enter the FQDNs or IP addresses of one or two NTP servers reachable from your network. If your Firewall Management Center does not have internet access you cannot use an NTP server outside of your local network.

Note
If you change network settings during initial configuration, you need to reconnect to the Firewall Management Center using the new network information.

Step 7 Click **Finish**.

The wizard performs validation on the values you enter on this screen to confirm syntactical correctness, compatibility of the entered values, and network connectivity between the Firewall Management Center and the DNS and NTP servers. If the system reports a connectivity problem after you click **Finish**, you cannot change the settings in the wizard, but you can configure these connections using the Firewall Management Center web interface after completing the initial setup.

What to do next

- The system displays a pop-up dialog box that offers you the opportunity to quickly and easily set up Smart Licensing. Using this dialog box is optional; if your Firewall Management Center Virtual will be managing Firewall Threat Defenses and you are familiar with Smart Licensing, use this dialog. Otherwise dismiss this dialog and refer to ”Licensing” in the *Cisco Secure Firewall Management Center Administration Guide* for your version.
- Review the weekly maintenance activites the Firewall Management Center configures automatically as a part of the initial configuration process. These activities are designed to keep your system up-to-date and your data backed up. See Review Automatic Initial Configuration for Versions 6.5 and Later, on page 7 .
- When you have completed the Initial Configuration Wizard and completed or dismissed the Smart Licensing dialog, the system displays the device management page, described in the *Cisco Secure Firewall Management Center Device Configuration Guide*.
- You can configure the Firewall Management Center for IPv6 addressing after completing the initial setup using the web interface as described in the *Cisco Secure Firewall Management Center Device Configuration Guide* for your version.

Review Automatic Initial Configuration for Versions 6.5 and Later

As a part of initial configuration (whether performed through the Initial Configuration Wizard or through the CLI), the Firewall 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. Also, because 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 Firewall Management Center has established them successfully, and adjust them if necessary.

- Weekly GeoDB Updates

  The Firewall Management Center automatically schedules GeoDB updates to occur each week at the same randomly selected time. You can observe the status of this update using the web interface Message

Center. You can see the configuration for this automatic update in the web interface under **System** > **Updates** > **Geolocation Updates**>**Recurring Geolocation Updates**. If the system fails to configure the update and your Firewall Management Center has internet access, we recommend you configure regular GeoDB updates as described in the *Cisco Secure Firewall Management Center Administration Guide* for your version.

- Weekly Firewall Management Center Software Updates

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

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

- Weekly Firewall Management Center Configuration Backup

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

- Vulnerability Database Update

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

- Daily Intrusion Rule Update

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