Cisco Firepower Management Center Virtual for VMware Setup

After you install a Cisco Firepower System virtual appliance, you must complete a setup process that allows the new appliance to communicate on your trusted management network. You must also change the administrator password and accept the end user license agreement (EULA).

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.

The purpose of these initial configurations and policies is to provide an out-of-the-box experience and to help you quickly set up your deployment, not to restrict your options. Regardless of how you initially configure a virtual appliance, you can change its configuration at any time using the Cisco Firepower Management Center. In other words, choosing a detection mode or access control policy during setup, for example, does not lock you into a specific device, zone, or policy configuration.

Regardless of how you deploy, begin by powering on the appliance to initialize it. After initialization completes, log in using the VMware console and complete the setup.

If you deploy with the VI OVF template, you can perform the network configuration using the wizard in the deployment. If you choose not to use the setup wizard or you deploy with the ESXi OVF template, configure network settings using a script. After your network is configured, complete the setup process using a computer on your management network to browse to the Cisco Firepower Management Center’s web interface.

Note: If you are deploying multiple appliances, set up your Firepower NGIPSv appliances 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.

Initializing a Virtual Appliance

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin</td>
</tr>
</tbody>
</table>

After you install a virtual appliance, initialization starts automatically when you power on the virtual appliance for the first time.

**Caution:** Startup time depends on a number of factors, including server resource availability. It can take up to 40 minutes for the initialization to complete. Do not interrupt the initialization or you may have to delete the appliance and begin again.

Use the following procedure to initialize a virtual appliance.

**Procedure**

1. Power on the appliance.
   - In the vSphere Client, right-click the name of your imported virtual appliance from the inventory list, then select **Power > Power On** from the context menu.
2. Monitor the initialization on the VMware console tab.
Setting Up a Cisco Firepower Management Center Virtual

The steps required to set up a Cisco Firepower Management Center Virtual depend on whether you deployed with a VI OVF template or an ESXi OVF template:

- If you deployed with a VI OVF template and used the setup wizard, log into the Firepower Management Center Virtual using the password you set when you configured the Firepower System-required settings, then use the Firepower System to set local appliance configurations, add licenses and devices, and apply policies to monitor and manage traffic. See the Firepower System Configuration Guide for more information.

- If you deployed with an ESXi OVF template or did not configure Firepower System-required settings when deploying with a VI OVF template deployment, setting up a Firepower Management Center Virtual is a two-step process. After you initialize the Firepower Management Center Virtual, run a script at the VMware console that helps you configure the appliance to communicate on your management network. Then, complete the setup process using a computer on your management network to browse to the appliance’s web interface.

- If you deploy the Firepower Management Center Virtual with the ESXi OVF template and deploy all the virtual devices with the VI OVF template, you can register all the devices at the same time to the Firepower Management Center Virtual through the one page setup wizard. See Initial Setup Page: Cisco Firepower Management Center Virtual, page 13 for more information.

Automating Firepower Management Center Virtual Network Settings

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Management Center</td>
<td>Global only</td>
<td>Admin</td>
</tr>
</tbody>
</table>

After you initialize a new Cisco Firepower Management Center Virtual, you must configure settings that allow the appliance to communicate on your management network. Complete this step by running a script at the VMware console.

The Firepower System provides a dual stack implementation for both IPv4 and IPv6 management environments. First, the script prompts you to configure (or disable) IPv4 management settings, then IPv6. For IPv6 deployments, you can retrieve settings from a local router. You must provide the IPv4 or IPv6 management IP address, netmask or prefix length, and default gateway.

When following the script’s prompts, for multiple-choice questions, your options are listed in parentheses, such as (y/n). Defaults are listed in square brackets, such as [y]. Press Enter to confirm a choice.

Before You Begin

Initialize the device as described in Initializing a Virtual Appliance, page 11.

Procedure

1. Log into the Firepower Management Center Virtual at the VMware console using admin as the username and the password for the admin account that you specified in the setup wizard when you deployed with a VI OVF template.

   If you did not change the password using the wizard, or you are deploying with an ESXi OVF template, use Admin123 as the password.

2. At the admin prompt, run the following script:

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

3. Follow the script’s prompts. First configure (or disable) IPv4 management settings, then IPv6. If you manually specify network settings, you must:
Setting Up a Cisco Firepower Management Center Virtual

— 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.

4. Confirm that your settings are correct.

If you entered settings incorrectly, type n at the prompt and press Enter. You can then enter the correct information. The VMware console may display messages as your settings are implemented.

5. Log out of the appliance.

What to Do Next

■ Continue with Initial Setup Page: Cisco Firepower Management Center Virtual, page 13 to complete the setup using the Cisco Firepower Management Center’s web interface.

Initial Setup Page: Cisco Firepower Management Center Virtual

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Management Center</td>
<td>Global only</td>
<td>Admin</td>
</tr>
</tbody>
</table>

For Cisco Firepower Management Center Virtual, you must complete the setup process by logging into the appliance’s web interface and specifying initial configuration options on a setup page. You must change the administrator password, specify network settings if you have not already, and accept the EULA.

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

Procedure

1. From a computer on your management network, direct a supported browser to https://MC_name/, where MC_name is the host name or IP address you assigned to the Firepower Management Center’s management interface in the previous procedure.

2. Log in using admin as the username and the password for the admin account that you specified in the setup wizard with a VI OVF template deployment. If you did not change the password using the wizard, use Admin123 as the password.

The setup page appears. See the following sections for information on completing the setup:

Change Password, page 14
Network Settings, page 14
Time Settings, page 14
Recurring Rule Update Imports, page 14
Recurring Geolocation Updates, page 15
Automatic Backups, page 15
License Settings, page 15
License Settings, page 15
End User License Agreement, page 16

3. When you are finished, click Apply.

The Firepower Management Center Virtual is configured according to your selections.
4. Use the Task Status page (System > Monitoring > Task Status) to verify that the initial setup was successful.

The page auto-refreshes every ten seconds. Monitor the page until it lists a status of Completed for any initial device registration and policy apply tasks. If, as part of setup, you configured an intrusion rule or geolocation update, you can also monitor those tasks.

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

What to Do Next

- Continue with Next Steps, page 17.

Change Password

You must change the password for the admin account. This account has Administrator privileges and cannot be deleted. Cisco recommends that you use a strong password that is at least eight alphanumeric characters of mixed case and includes at least one numeric character. Avoid using words that appear in a dictionary.

Network Settings

A Cisco Firepower Management Center’s network settings allow it to communicate on your management network. Because you already used a script to configure the network settings, this section of the page should be pre-populated.

If you want to change the pre-populated settings, remember that the Firepower System provides a dual stack implementation for both IPv4 and IPv6 management environments. You must specify the management network protocol (IPv4, IPv6, or Both). Depending on your choice, the setup page displays various fields where you must set the IPv4 or IPv6 management IP address, netmask or prefix length, and default gateway:

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

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

Time Settings

You can set the time for a Firepower Management Center either manually or via network time protocol (NTP) from an NTP server. You can also specify the time zone used on the local web interface for the admin account. Click the current time zone to change it using a pop-up window. Firepower Management Center

Note that any managed devices must be in time synchronization with the managing Firepower Management Center. Because the Firepower Management Center is not supported as an NTP source, we recommend that you use a physical NTP server to set your time.

Caution: If you set up a Firepower Management Center Virtual on VMware with manual time, it will (by default) take time from the host. Although you can configure an ESX/ESXi host as an NTP server, it is not a VMware best practice to do so. VMware considers it best practice to have your ESX/ESXi hosts configured to an authoritative time (NTP) server.

Recurring Rule Update Imports

As new vulnerabilities become known, the Cisco Vulnerability Research Team (VRT) releases intrusion rule updates. Rule updates provide new and updated intrusion rules and preprocessor rules, modified states for existing rules, and modified default intrusion policy settings. Rule updates may also delete rules and provide new rule categories and system variables.

If you plan to perform intrusion detection and prevention in your deployment, Cisco recommends that you Enable Recurring Rule Update Imports.
You can specify the **Import Frequency**, as well as configure the system to perform an intrusion **Policy Reapply** after each rule update. To perform a rule update as part of the initial configuration process, select **Install Now**.

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

### Recurring Geolocation Updates

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

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

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

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

### Automatic Backups

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

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

### License Settings

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

- For Firepower, ASA FirePOWER, and NGIPSv devices, you must use Classic Licenses.

By default, your Firepower Management Center can perform domain control, host, application, and user discovery, as well as decrypting and inspecting SSL- and TLS-encrypted traffic. Feature-specific classic licenses allow your managed devices to perform a variety of functions. For complete information about licensing, see the **Firepower System Configuration Guide** or the online help in the Firepower Management Center.

### Device Registration

A virtual Cisco Firepower Management Center can manage any device, physical or virtual, currently supported by the Firepower System. You can add most pre-registered devices to the Firepower Management Center during the initial setup process. However, if a device and the Firepower Management Center are separated by a NAT device, you must add it after the setup process completes.

When you register a managed device to a Firepower Management Center, leave the **Apply Default Access Control Policies** check box enabled if you want to automatically apply access control policies to devices upon registration. Note that you cannot choose which policy the Firepower Management Center applies to each device, only whether to apply them. The policy that is applied to each device depends on the detection mode you chose when configuring the device, as listed in the following table.
An exception occurs if you previously managed a device with a Firepower Management Center and you changed the device’s initial interface configuration. In this case, the policy applied by this new Firepower Management Center page depends on the changed (current) configuration of the device. If there are interfaces configured, the Firepower Management Center applies the Default Intrusion Prevention policy, otherwise, the Firepower Management Center applies the Default Access Control policy.

For more information on detection modes on virtual devices, see the *Cisco NGIPSv Quick Start Guide for VMware*; for physical devices, see the *Firepower System Installation Guide*.

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

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

Then, use the check boxes to add licensed capabilities to the device. Note that you can only select licenses you have already added to the Cisco Firepower Management Center. Also, you cannot enable certain licenses until you enable others. For example, you cannot enable Control on a device until you first enable Protection.

Because of architecture and resource limitations, not all licenses are supported on all managed devices. However, the setup page does not prevent you from enabling unsupported licenses on managed devices. This is because the Cisco Firepower Management Center does not determine the device model until later. The system cannot enable an invalid license, and attempting to enable an invalid license does not decrement your available license count.

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

### End User License Agreement

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

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

### Enabling VMware Tools

VMware Tools is a suite of utilities installed in the operating system of a virtual machine to enhance the performance of the virtual machine and to make possible many of the ease-of-use features of VMware products. The system supports the following plugins on all virtual appliances:

- guestInfo
- powerOps
Cisco Firepower Management Center Virtual for VMware Setup

Next Steps

- timeSync
- vmbackup
- snapshot

For more information on the supported plugins and full functionality of VMware Tools, see the VMware website (http://www.vmware.com/).

After you setup your virtual appliance, you can enable VMware Tools on your virtual appliances on your managed device using the command line interface (CLI) or on your virtual Firepower Management Center using your browser. For more information; see Configuring VMware Tools on a Firepower Management Center Virtual, page 17.

Configuring VMware Tools on a Firepower Management Center Virtual

You can select or clear a check box on the Configuration menu using the web interface. You cannot enable VMware Tools on a virtual Cisco Firepower Management Center using the CLI.

To enable or disable VMware Tools on a Cisco Firepower Management Center Virtual:

1. Using a web browser, log into your Cisco Firepower Management Center and select System > Configuration > VMware Tools, then select or clear the Enable VMware Tools check box and click Save.

Next Steps

After you complete the initial setup process for a virtual 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 of the tasks described in the following sections, as well as information on how you can begin to configure your deployment, see the Firepower System Configuration Guide.

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 Cisco 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.