Cisco Firepower Threat Defense Virtual for VMware Deployment

Revised: February 12, 2017

You can deploy the Cisco Firepower Threat Defense Virtual using VMware.

- Prerequisites for the Firepower Threat Defense Virtual and VMware, page 1
- Deploy the Firepower Threat Defense Virtual Using the VMware vSphere Web Client or vSphere Hypervisor, page 4
- Post-Installation Configuration, page 6
- Set Up a Firepower Threat Defense Virtual Device Using the CLI, page 9
- Register a Firepower Threat Defense Virtual to a Firepower Management Center, page 10

Prerequisites for the Firepower Threat Defense Virtual and VMware

You can deploy the Firepower Threat Defense Virtual using the VMware vSphere Web Client or the vSphere standalone client on ESXi. See Cisco Firepower Threat Defense Compatibility for system requirements.

Virtual appliances use e1000 (1 Gbit/s) interfaces by default. You can replace the default interfaces with vmxnet3 or ixgbe (10 Gbit/s) interfaces.

Modify the Security Policy Settings for a vSphere Standard Switch

For a vSphere standard switch, the three elements of the Layer 2 Security policy are promiscuous mode, MAC address changes, and forged transmits. Firepower Threat Defense Virtual uses promiscuous mode to operate, and Firepower Threat Defense Virtual high availability depends on switching the MAC address between the active and the standby to operate correctly.

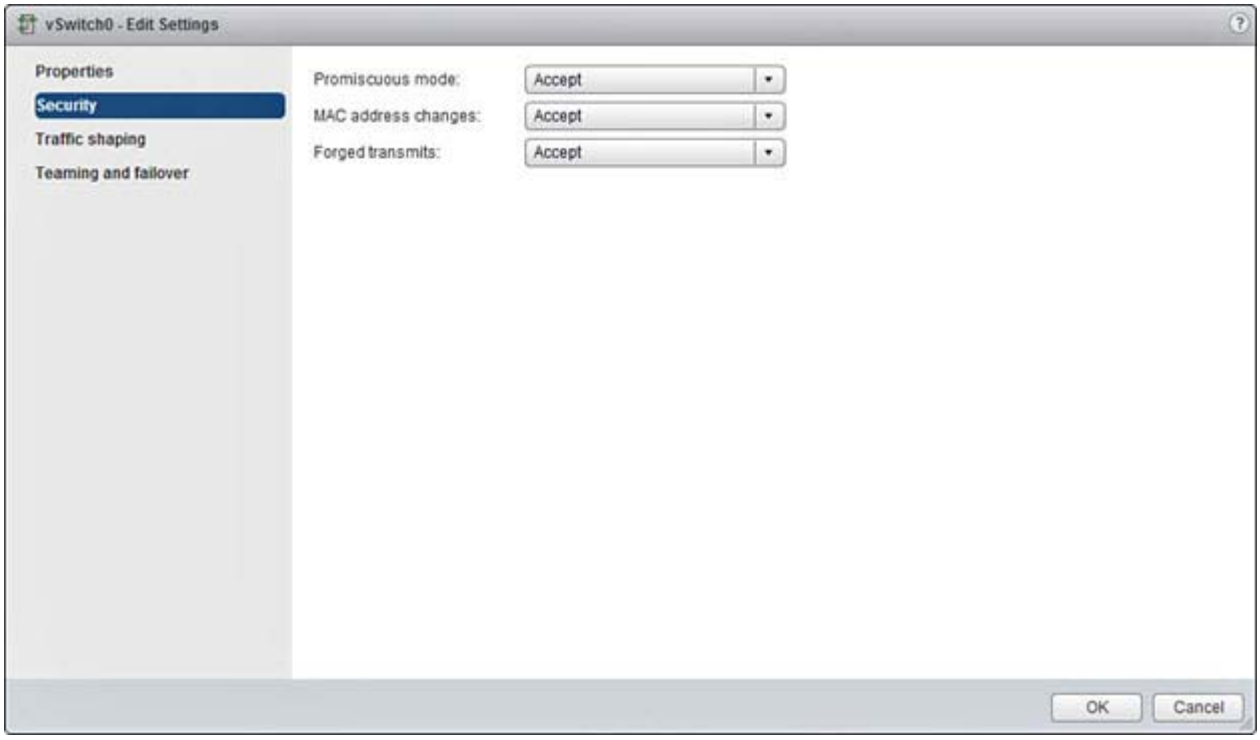
The default settings will block correct operation of Firepower Threat Defense Virtual. See the following required settings:

Table 1 vSphere Standard Switch Security Policy Options

Option	Required Setting	Action
Promiscuous Mode	Accept	You **must** edit the security policy for a vSphere standard switch in the vSphere Web Client and set the **Promiscuous mode** option to **Accept**. Firewalls, port scanners, intrusion detection systems and so on, need to run in promiscuous mode.
MAC Address Changes	Accept	You should verify the security policy for a vSphere standard switch in the vSphere Web Client and confirm the **MAC address changes** option is set to **Accept**.
Forged Transmits	Accept	You should verify the security policy for a vSphere standard switch in the vSphere Web Client and confirm the **Forged transmits** option is set to **Accept**.

Procedure

1. In the vSphere Web Client, navigate to the host.
2. On the **Manage** tab, click **Networking**, and select **Virtual switches**.
3. Select a standard switch from the list and click **Edit settings**.
4. Select **Security** and view the current settings.
5. **Accept** promiscuous mode activation, MAC address changes, and forged transmits in the guest operating system of the virtual machines attached to the standard switch.



6. Click **OK**.

What To do Next

Ensure these settings are the same on all networks that are configured for management and failover (HA) interfaces on Firepower Threat Defense Virtual sensors.

Guidelines for the Firepower Threat Defense Virtual and VMware

- The Firepower Threat Defense Virtual **must be powered up on firstboot with at least four interfaces**.
- The management interface (br1) for the e1000 driver is a bridged interface with two MAC addresses, one for management and one for diagnostics.
- The vmxnet3 driver uses two management interfaces. The first two Ethernet adapters must be configured as management interfaces; one for device management/registration (eth0), one for diagnotics (eth1).
- The ixgbe driver uses two management interfaces. The first two PCI devices must be configured as management interfaces; one for device management/registration (eth0), one for diagnotics (eth1).
- The only ixgbe traffic interface types supported in Version 6.0 are routed and ERSPAN passive. This is due to VMware limitations with respect to MAC address filtering.

  Note: The ixgbe driver does not support failover (HA) deployments of Firepower Threat Defense Virtual in this release.
- Cisco recommends using a host managed by VMware vCenter when using more than four vmxnet3 network cards. When deployed on standalone ESXi, additional network cards are not added to the virtual machine with sequential PCI bus addresses. See Adding and Configuring VMware Interfaces, page 7.
- vMotion is not supported.
- Cloning a virtual machine is not supported.
- Restoring a virtual machine with snapshot is not supported.
- Restoring a backup is not supported.

OVF File Guidelines

You have the following installation options for installing a Firepower Threat Defense Virtual appliance:

```
Cisco_Firepower_Threat_Defense_Virtual-VI-X.X.X-xxx.ovf
Cisco_Firepower_Threat_Defense_Virtual-ESXi-X.X.X-xxx.ovf
```

where *X.X.X-xxx* is the version and build number of the file you want to use.

- If you deploy with a VI OVF template, the installation process allows you to perform the entire initial setup for Firepower Threat Defense Virtual appliance. You can specify:
  - A new password for the admin account
  - Network settings that allow the appliance to communicate on your management network
  - The initial firewall mode
  - The managing Cisco Firepower Management Center

  Note: You must manage this virtual appliance using VMware vCenter.
- If you deploy using an ESXi OVF template, you must configure Firepower System-required settings after installation. You can manage this virtual appliance using VMware vCenter or use it as a standalone appliance; see Set Up a Firepower Threat Defense Virtual Device Using the CLI, page 9 for more information.

When you deploy an OVF template you provide the following information:

Table 2 VMware OVF Template

Setting	ESXi or VI	Action
Import/Deploy OVF Template	Both	Browse to the OVF templates you downloaded in the previous procedure to use.
OVF Template Details	Both	Confirm the appliance you are installing (Cisco Firepower Threat Defense Virtual) and the deployment option (`VI` or `ESXi`).
Accept EULA	VI only	Agree to accept the terms of the licenses included in the OVF template.
Name and Location	Both	Enter a unique, meaningful name for your virtual appliance and select the inventory location for your appliance.
Host / Cluster	Both	Select the host or cluster where you want to deploy the virtual appliance.
Resource Pool	Both	Manage your computing resources within a host or cluster by setting them up in a meaningful hierarchy. Virtual machines and child resource pools share the resources of the parent resource pool.
Storage	Both	Store all files associated with the virtual machines.
Disk Format	Both	Select the format to store the virtual disks: thick provision lazy zeroed, thick provision eager zeroed, or thin provision.
Network Mapping	Both	Select the management interface for the virtual appliance.
Properties	VI only	Customize the Virtual Machine initial configuration setup.

Deploy the Firepower Threat Defense Virtual Using the VMware vSphere Web Client or vSphere Hypervisor

You can use the VMware vSphere Web Client to deploy the Firepower Threat Defense Virtual. The Web Client requires vCenter. You can also use the vSphere Hypervisor for standalone ESXi deployment. You can use vSphere to deploy with either a VI OVF or ESXi OVF template:

- If you deploy using a VI OVF template, the appliance must be managed by VMware vCenter.
- If you deploy using a ESXi OVF template, the appliance can be managed by VMware vCenter or deployed to a standalone host. In either case, you must configure Firepower System-required settings after installation.

Before You Begin

- Download the archive file for Firepower Threat Defense Virtual from the Downloads area of the Cisco Support Site (https://software.cisco.com/ download/navigator.html).

  Note: A Cisco.com login and Cisco service contract are required.
- Unpack the archive file into a working directory. Do not remove any files from the directory.

Procedure

1. Using the vSphere Client, deploy the OVF template file you downloaded earlier by clicking **File** > **Deploy OVF Template**.
2. From the drop-down list, select one of the OVF templates you want to deploy for the Firepower Threat Defense Virtual device:

   ```
   Cisco_Firepower_Threat_Defense_Virtual-VI-X.X.X-xxx.ovf
   Cisco_Firepower_Threat_Defense_Virtual-ESXi-X.X.X-xxx.ovf
   ```

where *x.x.x-xxx* is the version and build number of the archive file you downloaded.

3. View the OVF Template Details page and click **Next**.
4. If license agreements are packaged with the OVF template (VI templates only), the End User License Agreement page appears. Agree to accept the terms of the licenses and click **Next**.
5. Optionally, edit the name and select the folder location within the inventory where the Firepower Threat Defense Virtual will reside, and click **Next**.

   Note: When the vSphere Client is connected directly to an ESXi host, the option to select the folder location does not appear.
6. Select the host or cluster on which you want to deploy the Firepower Threat Defense Virtual and click **Next**.
7. Navigate to, and select the resource pool where you want to run the Firepower Threat Defense Virtual and click **Next**.

   Note: This page appears only if the cluster contains a resource pool.
8. Select a storage location to store the virtual machine files, and click **Next**.

   On this page, you select from datastores already configured on the destination cluster or host. The virtual machine configuration file and virtual disk files are stored on the datastore. Select a datastore large enough to accommodate the virtual machine and all of its virtual disk files.
9. Select the disk format to store the virtual machine virtual disks, and click **Next**.

   When you select **Thick Provisioned**, all storage is immediately allocated. When you select **Thin Provisioned**, storage is allocated on demand as data is written to the virtual disks. Thin provisioning can also reduce the amount of time it takes to deploy the virtual appliance.
10. For each network specified in the OVF template, select a network by right-clicking the **Destination Networks** column in your infrastructure to set up the network mapping for each Firepower Threat Defense Virtual interface and click **Next**.

    Note: Firepower Threat Defense Virtual **requires** you to assign a network to **at least four interfaces**. Your system will not deploy without four interfaces.

    Ensure the Management0-0 interface is associated to a VM Network that is reachable from the Firepower Management Center. Non-management interfaces are configurable from the Firepower Management Center.

    The networks may not be in alphabetical order. If it is too difficult to find your networks, you can change the networks later from the Edit Settings dialog box. After you deploy, right-click the Firepower Threat Defense Virtual instance, and choose **Edit Settings** to access the **Edit Settings** dialog box. However that screen does not show the Firepower Threat Defense Virtual interface IDs (only Network Adapter IDs). See the following concordance of Source Networks and Destination Networks for Firepower Threat Defense Virtual interfaces:

Source Networks	Destination Networks	Function
Management0-0	Diagnostic0/0	Diagnostic and management
GigabitEthernet0-0	GigabitEthernet0/0	Traffic
GigabitEthernet0-1	GigabitEthernet0/1	Traffic
GigabitEthernet0-2	GigabitEthernet0/2	Traffic

After you deploy the Firepower Threat Defense Virtual, you can optionally return to the vSphere Client to add extra interfaces from the Edit Settings dialog box. You can have a total of 10 interfaces when you deploy a Firepower Threat Defense Virtual. For more information, see the vSphere Client online help.

Note: The vSphere Client REQUIRES you to assign a network to AT LEAST FOUR INTERFACES. You do not need to use all Firepower Threat Defense Virtual interfaces; for interfaces you do not intend to use, you can simply leave the interface disabled within the Firepower Threat Defense Virtual configuration.

11. If user-configurable properties are packaged with the OVF template (VI templates only), set the configurable properties and click **Next**.
12. Review and verify the settings on the **Ready to Complete** window. Optionally, check the **Power on after deployment** option to power on the Firepower Threat Defense Virtual, then click **Finish**.

    After you complete the wizard, the vSphere Web Client processes the VM; you can see the "Initialize OVF deployment" status in the **Global Information** area **Recent Tasks** pane.

    When it is finished, you see the Deploy OVF Template completion status.

    The Firepower Threat Defense Virtual VM instance then appears under the specified data center in the Inventory. Booting up the new VM could take up to 30 minutes.

    Note: To successfully register the Firepower Threat Defense Virtual with the Cisco Licensing Authority, the Firepower Threat Defense Virtual requires Internet access. You might need to perform additional configuration after deployment to achieve Internet access and successful license registration.

What To Do Next

- Determine if you need to modify the virtual appliance's hardware and memory settings, or configure interfaces; see Post-Installation Configuration, page 6.
- Register your Firepower Threat Defense Virtual to a Firepower Management Center; see Register a Firepower Threat Defense Virtual to a Firepower Management Center, page 10.

Post-Installation Configuration

After you deploy a virtual appliance, confirm that the virtual appliance's hardware and memory settings meet the requirements for your deployment. Do **not** decrease the default settings, as they are the minimum required to run the system software. The following table lists the default appliance settings.

Table 3 Default Virtual Appliance Settings

Setting	Default	Adjustable Setting?
memory	8GB	no
virtual CPUs	4	no
hard disk provisioned size	48.24GB	no, based on Disk Format selection (Thin Provision is 48.24GB)

Verifying Virtual Machine Properties

Use the VMware Virtual Machine Properties dialog box to verify the host resource allocation for the selected virtual machine. You can view CPU, memory, disk, and advanced CPU resources from this tab. You can also change the power-on connection setting, the MAC address, and the network connection for the virtual Ethernet adapter configuration for a virtual machine.

Procedure

1. Right-click the name of your new virtual appliance, then select **Edit Settings** from the context menu, or click **Edit virtual machine settings** from the **Getting Started** tab in the main window.
2. Make sure the **Memory**, **CPUs**, and **Hard disk 1** settings are set to the defaults, as described in Table 3 Default Virtual Appliance Settings, page 6.

   The memory setting and the number of virtual CPUs for the appliance are listed on the left side of the window. To see the hard disk **Provisioned Size**, click **Hard disk 1**.
3. Confirm the **Network adapter 1** settings are as follows, making changes if necessary:
   a. Under **Device Status**, enable the **Connect at power on** check box.
   b. Under **MAC Address**, manually set the MAC address for your virtual appliance's management interface.

      Manually assign the MAC address to your virtual appliance to avoid MAC address changes or conflicts from other systems in the dynamic pool.

      Additionally, for virtual Cisco Firepower Management Centers, setting the MAC address manually ensures that you will not have to re-request licenses from Cisco if you ever have to reimage the appliance.
   c. Under **Network Connection**, set the **Network label** to the name of the management network for your virtual appliance.
4. Click **OK**.

What to Do Next

- Initialize the virtual appliance; see Initializing a Virtual Appliance, page 8.
- Optionally, before you power on the appliance, you can replace the default e1000 interfaces with vmxnet3 interfaces, create an additional management interface, or both; see Adding and Configuring VMware Interfaces, page 7.

Adding and Configuring VMware Interfaces

VMware defaults to e1000 (1 Gbit/s) interfaces when it creates a virtual machine. Once the virtual machine is finished and the Firepower Threat Defense Virtual is installed fully you can switch from the e1000 to either vmxnet3 (10 Gbit/s) or ixgbe (10 Gbit/s) interfaces for greater network throughput. The following guidelines are important when replacing the default e1000 interfaces:

- For vmxnet3, Cisco recommends using a host managed by VMware vCenter when using more than four vmxnet3 network interfaces. When deployed on standalone ESXi, additional network interfaces are not added to the virtual machine with sequential PCI bus addresses. When the host is managed with a VMware vCenter, the correct order can be obtained from the XML in the configuration CDROM. When the host is running standalone ESXi, the only way to determine the order of the network interfaces is to manually compare the MAC addresses seen on the Firepower Threat Defense Virtual to the MAC addresses seen from the VMware configuration tool.
- The vmxnet3 driver uses two management interfaces. The first two Ethernet adapters must be configured as management interfaces; one for device management/registration, one for diagnotics.
- For ixgbe, the ESXi platform requires the ixgbe NIC to support the ixgbe PCI device. In addition, the ESXi platform has specific BIOS and configuration requirements that are needed to support ixgbe PCI devices. Refer to the Intel Technical Brief *How to Configure Intel® Ethernet Converged Network Adapter-Enabled Virtual Functions on VMware* ESXi* 5.1* for more information.

- The ixgbe driver uses two management interfaces. The first two PCI devices must be configured as management interfaces; one for device management/registration, one for diagnotics.

  Note: The ixgbe driver does not support failover (HA) deployments of Firepower Threat Defense Virtual in this release.

You can replace the default e1000 interfaces by deleting all of the e1000 interfaces and replacing them with vmxnet3 or ixgbe interfaces.

Although you can mix interfaces in your deployment (such as, e1000 interfaces on a virtual Cisco Firepower Management Center and vmxnet3 interfaces on its managed virtual device), you cannot mix interfaces on the same appliance. All sensing and management interfaces on the appliance must be of the same type.

To replace e1000 interfaces, use the vSphere Client to first remove the existing e1000 interfaces, add the new interfaces, and then select the appropriate adapter type and network connection.

You can also add an additional management interface on the same virtual Firepower Management Center to manage traffic separately on two different networks. Configure an additional virtual switch to connect the second management interface to a managed device on the second network. Use the vSphere Client to add a second management interface to your virtual appliance.

Note: Make all changes to your interfaces before you turn on your appliance. To change the interfaces, you must power down the appliance, delete the interfaces, add the new interfaces, then power on the appliance.

For more information about using the vSphere Client, see the VMware website (http://vmware.com). For more information about multiple management interfaces, see Managing Devices in the *Firepower Management Center Configuration Guide*.

Initializing a Virtual Appliance

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.

What to Do Next

- If you used a VI OVF template and configured your Firepower System-required settings during deployment, no further configuration is required; see Register a Firepower Threat Defense Virtual to a Firepower Management Center, page 10.
- If you used an ESXi OVF template or you did not configure Firepower System-required settings when you deployed with the VI OVF template, continue with Set Up a Firepower Threat Defense Virtual Device Using the CLI, page 9.

Set Up a Firepower Threat Defense Virtual Device Using the CLI

Because Firepower Threat Defense Virtual appliances do not have web interfaces, you must set up a virtual device using the CLI if you deployed with an ESXi OVF template. You can also use the CLI to configure Firepower System-required settings if you deployed with a VI OVF template and did not use the setup wizard during deployment.

Note: If you deployed with a VI OVF template and used the setup wizard, your virtual device is configured and no further action is required.

When you first log into a newly configured device, you must read and accept the EULA. Then, follow the setup prompts to change the administrator password, and configure the device's network settings and firewall mode.

When following the setup 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.

Note that the CLI prompts you for much of the same setup information that a physical device's setup web page does. For more information, see the *Firepower System Installation Guide*.

Note: To change any of these settings for a virtual device after you complete the initial setup, you must use the CLI. For more information, see the Command Line Reference chapter in the *Firepower Management Center Configuration Guide*.

Procedure

1. Open the VMware console.
2. Log into the virtual appliance at the VMware console using `admin` as the username and the new admin account password that you specified in the deployment setup wizard.

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

   The device immediately prompts you to read the EULA.
3. Read and accept the EULA.
4. Change the password for the `admin` account. This account has the Configuration CLI access level, and cannot be deleted.

   Note: 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.
5. Complete the system configuration as prompted.

   The VMware console may display messages as your settings are implemented. When finished, the device reminds you to register this device to a Cisco Firepower Management Center, and displays the CLI prompt.
6. Verify the setup was successful when the console returns to the firepower **#** prompt.

   Note: To successfully register the Firepower Threat Defense Virtual with the Cisco Licensing Authority, the Firepower Threat Defense Virtual requires Internet access. You might need to perform additional configuration after deployment to achieve Internet access and successful license registration.

What to Do Next

- Register your Firepower Threat Defense Virtual to a Firepower Management Center; see Register a Firepower Threat Defense Virtual to a Firepower Management Center, page 10.

Register a Firepower Threat Defense Virtual to a Firepower Management Center

Because virtual devices do not have web interfaces, you must use the CLI to register a virtual device to a Cisco Firepower Management Center, which can be physical or virtual. 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 self-generated alphanumeric registration key is always required to register a device to a Firepower Management Center. This is a simple key that you specify, and it is not the same as a license key.

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

`configure manager add` *`XXX.XXX.XXX.XXX my_reg_key`*

where *`XXX.XXX.XXX.XXX`* is the IP address of the managing Firepower Management Center and *`my_reg_key`* is the registration key you entered for the virtual device.

Note: On the ESXi platform, when using the vSphere Client to register a virtual device to a Firepower Management Center, you must use the IP address (not the hostname) of the managing Firepower Management Center if DNS information is not provided during the setup.

However, if the device and the Firepower Management Center are separated by a Network Address Translation (NAT) device, and the Firepower Management Center is behind a NAT device, enter a unique NAT ID along with the registration key, and specify `DONTRESOLVE` instead of the IP address. For example:

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

where *`my_reg_key`* is the registration key you entered for the virtual device and *`my_nat_id`* is the NAT ID of the NAT device.

If the device, rather than the Firepower Management Center, is behind a NAT device, enter a unique NAT ID along with the registration key, and specify the host name or IP address of the Firepower Management Center. For example:

`configure manager add [hostname | ip address]` *`my_reg_key my_nat_id`*

where *`my_reg_key`* is the registration key you entered for the virtual device and *`my_nat_id`* is the NAT ID of the NAT device.

Procedure

1. Log into the virtual device as a user with CLI Configuration (Administrator) privileges:
   - If you are performing the initial setup from the VMware console, you are already logged in as the `admin` user, which has the required access level.
   - Otherwise, log into the device using the VMware console, or, if you have already configured network settings for the device, SSH to the device's management IP address or host name.
2. At the prompt, register the device to a Cisco 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 the 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 required to register a device to the Firepower Management Center.

Note: The registration key is a user-generated one-time use key that must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). You will need to remember this registration key when you add the device to the Firepower Management Center.

- *nat_id* is an optional alphanumeric string used during the registration process between the Cisco Firepower Management Center and the device. It is required if the hostname is set to `DONTRESOLVE`.

Note: Use the `show managers` command to monitor the state of the device registration.

3. Log out of the appliance.

What to Do Next

- Log into its web interface and use the Device Management (**Devices > Device Management**) page to add the device if you have already set up the Firepower Management Center. For more information, see the Managing Devices chapter in the *Firepower Management Center Configuration Guide*.