Installing Virtual Appliances

Cisco provides packaged virtual appliances for VMware ESXi host environments on its Support Site as compressed archive (`.tar.gz`) files. Cisco virtual appliances are packaged as virtual machines with Version 7 of the virtual hardware.

You deploy a virtual appliance with a virtual infrastructure (VI) or ESXi Open Virtual Format (OVF) template:

- When you deploy with a VI OVF template, you can configure FireSIGHT System-required settings (such as the password for the admin account and settings that allow the appliance to communicate on your network) using the setup wizard in the deployment.
- You must deploy to a managing platform, either VMware vCloud Director or VMware vCenter.
- When you deploy with an ESXi OVF template, you must configure settings after installation using the command line interface (CLI) on the VMware console of the virtual appliance.
- You can deploy to a managing platform (VMware vCloud Director or VMware vCenter), or you can deploy as a standalone appliance.

Note VMware snapshots of Cisco virtual appliances are **not** supported.

Use the instructions in this chapter to download, install, and configure a Cisco virtual appliance. For help creating a virtual host environment, see the VMware ESXi documentation.

After you install and configure a virtual appliance according to the following procedures, power it on to initialize it and begin the initial setup process as described in the next chapter. For information on uninstalling a virtual appliance, see Uninstalling a Virtual Appliance, page 4-11.

To install and deploy a Cisco virtual appliance:

Step 1 Make sure your planned deployment meets the prerequisites described in Operating Environment Prerequisites, page 1-5.

Step 2 Obtain the correct archive files from the Support Site, copy them to an appropriate storage medium, and decompress them; see Obtaining the Installation Files, page 4-2.

Step 3 Use the VMware vCloud Director web portal or vSphere Client to install the virtual appliance, but do not power it on; see Installing a Virtual Appliance, page 4-3.

Step 4 Confirm and adjust network, hardware, and memory settings; see Updating Important Settings Post-Installation, page 4-8.

Step 5 Optionally, replace the default e1000 interfaces with vmxnet3 interfaces, create an additional management interface, or both. For more information, see Adding and Configuring Interfaces, page 4-9.

Step 6 Make sure the sensing interfaces on virtual devices are correctly connected to an ESXi host virtual switch; see Configuring Virtual Device Sensing Interfaces, page 4-10.

Obtaining the Installation Files

Cisco provides compressed archive (`.tar.gz`) files for installing virtual appliances: one for Defense Centers and one for devices. Each archive contains the following files:

- an Open Virtual Format (`.ovf`) template containing `-ESXi-` in the file name
- an Open Virtual Format (`.ovf`) template containing `-VI-` in the file name
- a Manifest File (`.mf`) containing `-ESXi-` in the file name
- a Manifest File (`.mf`) containing `-VI-` in the file name
- the Virtual Machine Disk Format (`.vmdk`)

Before you install a virtual appliance, obtain the correct archive file from the Support Site. Cisco recommends that you always use the most recent package available. Virtual appliance packages are usually associated with major versions of the system software (for example, 5.3 or 5.4).

To obtain virtual appliance archive files:

Step 1 Using the user name and password for your support account, log into the Support Site (https://support.sourcefire.com/).

Step 2 Click **Downloads**, select the **3D System** tab on the page that appears, and then click the major version of the system software you want to install.

For example, to download a Version 5.4.1 archive file, click **Downloads > 3D System > 5.4.1**.

Step 3 Find the archive file that you want to download for either the virtual device or virtual Defense Center, using the following naming convention:

```
Sourcefire_3D_Device_Virtual64_VMware-X.X.X-xxx.tar.gz
Sourcefire_Defense_Center_Virtual64_VMware-X.X.X-xxx.tar.gz
```

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

You can click one of the links on the left side of the page to view the appropriate section of the page. For example, click **5.4.1 Virtual Appliances** to view the archive files for Version 5.4.1 of the FireSIGHT System.

Step 4 Click the archive you want to download.

The file begins downloading.

Tip While you are logged into the Support Site, Cisco recommends you download any available updates for virtual appliances so that after you install a virtual appliance to a major version, you can update its system software. You should always run the latest version of the system software supported by your appliance. For Defense Centers, you should also download any new intrusion rule and Vulnerability Database (VDB) updates.

Step 5 Copy the archive file to a location accessible to the workstation or server that is running the vSphere Client or VMware vCloud Director web portal.

Caution Do **not** transfer archive files via email; the files can become corrupted.

Step 6 Decompress the archive file using your preferred tool and extract the installation files.

For the virtual device:

```
Sourcefire_3D_Device_Virtual64_VMware-X.X.X-xxx-disk1.vmdk
Sourcefire_3D_Device_Virtual64_VMware-ESXi-X.X.X-xxx.ovf
Sourcefire_3D_Device_Virtual64_VMware-ESXi-X.X.X-xxx.mf
Sourcefire_3D_Device_Virtual64_VMware-VI-X.X.X-xxx.ovf
Sourcefire_3D_Device_Virtual64_VMware-VI-X.X.X-xxx.mf
```

For the virtual Defense Center:

```
Sourcefire_Defense_Center_Virtual64_VMware-X.X.X-xxx-disk1.vmdk
Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.X-xxx.ovf
Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.X-xxx.mf
Sourcefire_Defense_Center_Virtual64_VMware-VI-X.X.X-xxx.ovf
Sourcefire_Defense_Center_Virtual64_VMware-VI-X.X.X-xxx.mf
```

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

Make sure you keep all the files in the same directory.

Step 7 Continue with Installing a Virtual Appliance to deploy the virtual appliance.

Installing a Virtual Appliance

To install a virtual appliance, you deploy an OVF (VI or ESXi) template to a managing platform (VMware vCloud Director or VMware vCenter) using a platform interface (VMware vCloud Director web portal or vSphere Client):

- If you deploy using a VI OVF template, you can configure FireSIGHT System-required settings during installation. You must manage this virtual appliance using either VMware vCloud Director or VMware vCenter.
- If you deploy using an ESXi OVF template, you must configure FireSIGHT System-required settings after installation. You can manage this virtual appliance using either VMware vCloud Director or VMware vCenter, or use it as a standalone appliance.

After you make sure your planned deployment meets the prerequisites (described in Operating Environment Prerequisites, page 1-5) and download the necessary archive files, use the VMware vCloud Director web portal or vSphere Client to install virtual appliances.

You have the following installation options for installing a virtual appliance:

- For a virtual Defense Center:

  ```
  Sourcefire_Defense_Center_Virtual64_VMware-VI-X.X.X-xxx.ovf
  Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.X-xxx.ovf
  ```

- For the virtual device:

  ```
  Sourcefire_3D_Device_Virtual64_VMware-VI-X.X.X-xxx.ovf
  ```

```
Sourcefire_3D_Device_Virtual64_VMware-ESXi-X.X.X-xxx.ovf
```

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

The following table lists the information required for deployment:

Table 4-1 VMware OVF Template

Setting	Action
Import/Deploy OVF Template	Browse to the OVF templates you downloaded in the previous procedure to use.
OVF Template Details	Confirm the appliance you are installing (virtual Defense Center or virtual device) and the deployment option (`VI` or `ESXi`).
Name and Location	Enter a unique, meaningful name for your virtual appliance and select the inventory location for your appliance.
Host / Cluster	For virtual devices only, select the host or cluster where you want to deploy the device.
Disk Format	Select the format to store the virtual disks: thick provision lazy zeroed, thick provision eager zeroed, or thin provision.
Network Mapping	Select the management interface for the virtual appliance.

If you deploy with a VI OVF template, the installation process allows you to perform basic setup for virtual Defense Centers and the entire initial setup for virtual devices. You can specify:

- a new password for the admin account
- network settings that allow the appliance to communicate on your management network
- for virtual devices only, the initial detection mode
- for virtual devices only, the managing Defense Center

If you deploy with an ESXi OVF template or if you choose not to configure with the setup wizard, you must perform the initial setup for virtual appliances using the VMware console. For detailed information on performing the initial setup, including guidance on what configurations to specify, see Setting Up Virtual Appliances, page 5-1.

Use one of the following options to install your virtual appliance:

- Installing with the VMware vCloud Director Web Portal, page 4-4 describes how to deploy a virtual appliance to the VMware vCloud Director.
- Installing with vSphere Client, page 4-6 describes how to deploy a virtual appliance to the VMware vCenter.

To understand network settings and detection modes, see Setting Up a Virtual Device Using the CLI, page 5-3 and Setting Up a Virtual Defense Center, page 5-6.

Installing with the VMware vCloud Director Web Portal

You can use VMware vCloud Director web portal to deploy a virtual appliance using the following steps:

- Create an organization and catalog to contain the vApp templates. For more information, see the *VMware vCloud Director User's Guide*.

- Upload the FireSIGHT System virtual appliance OVF packages to the catalog as vApp templates. For more information, see Uploading the Virtual Appliance OVF Packages, page 4-5.
- Create a virtual appliance using a vApp template. For more information, see Using the vApp Template, page 4-5.

Uploading the Virtual Appliance OVF Packages

You can upload the following OVF packages the following OVF packages to your VMware vCloud Director organization catalog:

For the virtual Defense Center:

`Sourcefire_Defense_Center_Virtual64_VMware-VI-X.X.X-  xxx.ovf`

For the virtual device:

`Sourcefire_3D_Device_Virtual64_VMware-VI-X.X.X-xxx.ovf`

where *X.X.X-xxx* is the version and build number of the OVF package you want to upload.

To upload the virtual appliance OVF packages:

Step 1 On the VMware vCloud Director web portal, select **Catalogs >** *Organization* **> vApp Templates** where *Organization* is the name of the organization that you want to contain your vApp templates.

Step 2 On the vApp Templates media tab, click the Upload icon ( ).

The Upload OVF package as a vApp Template pop-up window appears.

Step 3 In the OVF package field, enter the location of the OVF package, or click **Browse** to browse to the OVF package:

- For the virtual Defense Center:

  `Sourcefire_Defense_Center_Virtual64_VMware-VI-X.X.X-xxx.ovf`

- For the virtual device:

  `Sourcefire_3D_Device_Virtual64_VMware-VI-X.X.X-xxx.ovf`

- where *X.X.X-xxx* is the version and build number of the OVF package you want to upload.

Step 4 Enter a name and optionally a description for the OVF package.

Step 5 From the drop-down lists, select the virtual datacenter, storage profile, and catalog to contain the vApp template.

Step 6 Click **Upload** to upload the OVF package as a vApp template to the catalog.

The OVF package uploads to your organization's catalog.

Step 7 Continue with Using the vApp Template to create a virtual appliance from the vApp template.

Using the vApp Template

You can use a vApp template to create a virtual appliance allows you to configure FireSIGHT System-required settings during the installation using a setup wizard. After you specify settings on each page of the wizard, click **Next** to continue. For your convenience, the final page of the wizard allows you to confirm your settings before completing the procedure.

To use the vApp template to create a virtual appliance:

Step 1 On the VMware vCloud Director web portal, select **My Cloud > vApps**.

Step 2 On the vApps media tab, click the Add icon ( ) to add a vApp from the catalog.

The Add vApp from Catalog pop-up window appears.

Step 3 Click **All Templates** on the template menu bar.

A list of all available vApp templates is displayed.

Step 4 Select the vApp template you want to add to display a description of the virtual appliance.

- For the virtual Defense Center:

  `Sourcefire_Defense_Center_Virtual64_VMware-VI-X.X.X-xxx.ovf`

- For the virtual device:

  `Sourcefire_3D_Device_Virtual64_VMware-VI-X.X.X-xxx.ovf`

- where *X.X.X-xxx* is the version and build number of the archive file.

The End User License Agreement (EULA) appears.

Step 5 Read and accept the EULA.

The Name this vApp screen appears.

Step 6 Enter a name and optionally a description for the vApp.

The Configure Resources screen appears.

Step 7 On the Configure Resources screen, select the virtual datacenter, enter a computer name (or using the default computer name), and select the storage profile.

The Network Mapping screen appears.

Step 8 Map the networks used in the OVF template to a network in your inventory by selecting the destination for the external, management, and internal sources, and your IP allocation.

The Custom Properties screen appears.

Step 9 Optionally, on the Custom Properties screen, perform the initial setup for the appliance by entering the FireSIGHT System-required settings on the setup wizard. If you do not perform the initial setup now, you can do it later using the instructions in Setting Up Virtual Appliances, page 5-1.

The Ready to Complete screen appears, which displays the configuration for your virtual appliance.

Step 10 Confirm your settings and click **Finish**.

Note Do **not** enable the **Power on after deployment** option for a virtual device. You must map your sensing interfaces and be sure they are set to connect before powering on the appliance. For more information, see Initializing a Virtual Appliance, page 5-2.

Step 11 Continue with Updating Important Settings Post-Installation, page 4-8.

Installing with vSphere Client

You can use the vSphere Client 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 or VMware vCloud Director.
- If you deploy using a ESXi OVF template, the appliance can be managed by VMware vCenter, VMware vCloud Director, or deployed to a standalone host. In either case, you must configure FireSIGHT System-required settings after installation.

After you specify settings on each page of the wizard, click **Next** to continue. For your convenience, the final page of the wizard allows you to confirm your settings before completing the procedure.

To install a virtual appliance using vSphere Client:

Step 1 Using the vSphere Client, deploy the OVF template file you downloaded earlier by clicking **File > Deploy OVF Template**.

The Source screen appears, where you can browse through a drop-down list for the template you want to deploy.

Step 2 From the drop-down list, select the OVF template you want to deploy:

- For the virtual Defense Center:

```
Sourcefire_Defense_Center_Virtual64_VMware-VI-X.X.X-xxx.ovf
Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.X-xxx.ovf
```

- For the virtual device:

```
Sourcefire_3D_Device_Virtual64_VMware-VI-X.X.X-xxx.ovf
Sourcefire_3D_Device_Virtual64_VMware-ESXi-X.X.X-xxx.ovf
```

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

The OVF Template Details screen appears.

Step 3 Confirm that you selected the correct virtual machine:

- For the ESXi OVF template:
- The Name and Location screen appears.
- For the VI OVF template:
- The End User License Agreement (EULA) screen appears.
- Read and accept the EULA, then the Name and Location screen appears.

Step 4 Type the name for your virtual appliance in the text field, and select the inventory location for where you want to deploy the appliance.

The Host / Cluster screen appears.

Step 5 Select the host or cluster where you want to deploy the template.

The Specific Host screen appears.

Step 6 Select the specific host within the cluster where you want to deploy the template.

The Storage screen appears.

Step 7 Select the destination storage for the virtual machine.

The Disk Format screen appears.

Step 8 Select which format you want to store the virtual disks from the following options:

- thick provision lazy zeroed
- thin provision eager zeroed

- thin provision

The Network Mapping screen appears.

Step 9 Select the network where you want to deploy the template:

- For the ESXi OVF template:
- The ESXi Finish screen appears.
- For the VI OVF template:
- The Properties screen appears.
- Enter the FireSIGHT System-required settings for the appliance or click through to complete the setup later, confirm your settings, then click **Finish**.

Note Do **not** enable the **Power on after deployment** option for a virtual device. You must map your sensing interfaces and be sure they are set to connect before powering on the appliance. For more information, see Initializing a Virtual Appliance, page 5-2.

Step 10 After the installation is complete, close the status window.

Step 11 Continue with Updating Important Settings Post-Installation.

Updating Important Settings Post-Installation

After you install a virtual appliance, you must 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. However, to improve performance, you can increase a virtual appliance's memory and number of CPUs, depending on your available resources. The following table lists the default appliance settings.

Table 4-2 Default Virtual Appliance Settings

Setting	Default	Adjustable Setting?
memory	4GB	yes, and for a virtual device you **must** allocate: • 4GB minimum • 5GB to add category and reputation-based URL filtering • 6GB to add Security Intelligence filtering using large dynamic feeds • 7GB to add URL filtering and Security Intelligence
virtual CPUs	4	yes, up to 8
hard disk provisioned size	40GB (device) 250GB (Defense Center)	no

The following procedure explains how to check and adjust a virtual appliance's hardware and memory settings.

To check your virtual appliance settings:

Step 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.

The Virtual Machine Properties pop-up window appears, displaying the Hardware tab.

Step 2 Make sure the **Memory**, **CPUs**, and **Hard disk 1** settings are set no lower than the defaults, as described in Table 4-2Default Virtual Appliance Settings, page 4-8.

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**.

Step 3 Optionally, increase the memory and number of virtual CPUs by clicking the appropriate setting on the left side of the window, then making changes on the right side of the window.

Step 4 Confirm the **Network adapter 1** settings are as follows, making changes if necessary:

- Under **Device Status**, enable the **Connect at power on** check box.
- Under **MAC Address**, manually set the MAC address for your virtual appliance's management interface.
- Manually assign the MAC address to your virtual device to avoid MAC address changes or conflicts from other systems in the dynamic pool.
- Additionally, for virtual Defense Centers, setting its MAC address manually ensures that you will not have to re-request licenses from Cisco if you ever have to reimage the appliance.
- Under **Network Connection**, set the **Network label** to the name of the management network for your virtual appliance.

Step 5 Click **OK**.

Your changes are saved.

Step 6 Optionally, before you power on the appliance, you can replace the default e1000 interfaces with vmxnet3 interfaces, create an additional management interface, or both. For more information, see Adding and Configuring Interfaces, page 4-9.

Step 7 The next step depends on the type of appliance you just installed:

- A virtual Defense Center is ready to initialize: continue with Setting Up Virtual Appliances, page 5-1.
- A virtual device needs some additional configurations: continue with Configuring Virtual Device Sensing Interfaces.

Adding and Configuring Interfaces

You can replace the default e1000 (1 Gbit/s) interfaces with vmxnet3 (10 Gbit/s) interfaces by deleting all of the e1000 interfaces and replacing them with vmxnet3 interfaces.

Although you can mix interfaces in your deployment (such as, e1000 interfaces on a virtual Defense 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 the same, either e1000 or vmxnet3.

To replace e1000 interfaces with vmxnet3 interfaces, use the vSphere Client to first remove the existing e1000 interfaces, add the new vmxnet3 interfaces, and then select the appropriate adapter type and network connection.

You can also add a second management interface on the same virtual Defense 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.

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 FireSIGHT System User Guide.

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

Configuring Virtual Device Sensing Interfaces

The sensing interfaces on a virtual device must have a network connection to a port on an ESXi host virtual switch that accepts promiscuous mode.

Tip Add a port group to a virtual switch to isolate promiscuous mode virtual network connections from your production traffic. For information on adding port groups and setting security attributes, see your VMware documentation.

To permit promiscuous mode:

Step 1 Use the vSphere Client to log into your server and click on your server's **Configuration** tab.

The **Hardware** and **Software** selection lists appear.

Step 2 In the **Hardware** list, click **Networking**.

The virtual switch diagram appears.

Step 3 On the switch and port group where you connect the sensing interfaces of the virtual device, click **Properties**.

The **Switch Properties** pop-up window appears.

Step 4 On the **Switch Properties** pop-up window, click **Edit**.

The **Detailed Properties** pop-up window appears.

Step 5 On the **Detailed Properties** pop-up window, select the **Security** tab.

Under **Policy Exceptions > Promiscuous Mode**, confirm that the Promiscuous Mode is set to **Accept**.

Tip To monitor VLAN traffic in your virtual environment, set the VLAN ID of the promiscuous port to 4095.

Step 6 Save your changes.

The device is ready to initialize.

Step 7 Continue with the next chapter, Setting Up Virtual Appliances, page 5-1.

Uninstalling a Virtual Appliance

You may need to uninstall or remove your virtual appliances. Shut down the virtual appliance, then uninstall a virtual appliance by deleting it.

Tip After you remove the virtual device, remember to return the sensing connections virtual switch port group to the default setting: **Promiscuous Mode**: **Reject**. For more information, see Configuring Virtual Device Sensing Interfaces, page 4-10.

Shutting Down a Virtual Appliance

Use the following procedure to properly shut down a virtual appliance.

To shut down a virtual appliance:

Step 1 At the VMware console, log in as a user with Administrator (or, for virtual devices, CLI Configuration) privileges. If you are using a virtual device, type `expert` to display the shell prompt.

The prompt for the appliance appears.

Step 2 Shut down the virtual appliance:

- On a virtual Defense Center, type `sudo shutdown -h now`.
- On a virtual device, type `system shutdown`.

The virtual appliance shuts down.

Deleting a Virtual Appliance

After the virtual appliance powers off, you can delete the virtual appliance.

Use the following procedure to delete a virtual appliance deployed on VMware vCloud Director:

To delete the virtual appliance using VMware vCloud Director web portal:

Step 1 Select **My Cloud > vApps**, right-click on the vApp you want to delete and click **Delete** from the menu, then click **Yes** on the confirmation pop-up window.

The virtual appliance is uninstalled.

Use the following procedure to delete a virtual appliance deployed on VMware vCenter:

To delete a virtual appliance using the vSphere Client:

Step 1 Click on name of the appliance in the vSphere Client context menu and click **Delete** using the Inventory menu, then click **Yes** in the confirmation dialog box.

The virtual appliance is uninstalled.