Deploy the Firewall Management Center Virtual on VMware

You can deploy the Firewall Management Center Virtual using VMware.

VMware Feature Support for the Firewall Management Center Virtual

The following table lists the VMware feature support for the Firewall Management Center Virtual.

Table 1: VMware Feature Support for the Firewall Management Center Virtual

Feature	Description	Support (Yes/No)	Comment
Cold Clone	The VM is powered off during cloning.	No	–
Hot add	The VM is running during an addition.	No	–
Hot clone	The VM is running during cloning.	No	–
Hot removal	The VM is running during removal.	No	–

Feature	Description	Support (Yes/No)	Comment
Snapshots	The VM freezes for a few seconds.	No	There is a risk of out-of-sync situations between the FMC and managed devices. See Snapshots Support, on page 7 .
Suspend and resume	The VM is suspended, then resumed.	Yes	–
vCloud Director	Allows automatic deployment of VMs.	No	–
VM migration	The VM is powered off during migration.	Yes	–
vMotion	Used for live migration of VMs.	Yes	Use shared storage. See vMotion Support, on page 7.
VMware FT	Used for HA on VMs.	No	–
VMware HA	Used for ESXi and server failures.	Yes	–
VMware HA with VM heartbeats	Used for VM failures.	No	–
VMware vSphere Standalone Windows Client	Used to deploy VMs.	Yes	–
VMware vSphere Web Client	Used to deploy VMs.	Yes	–

System Requirements

Firewall Management Center Virtual Requires 28 GB RAM for Upgrade (6.6.0+)

The Firewall Management Center Virtual platform has introduced a new memory check during upgrade. The Firewall Management Center Virtual upgrades to Version 6.6.0+ will fail if you allocate less than 28 GB RAM to the virtual appliance.

Important We recommend you do not decrease the default settings: 32 GB RAM for most of the Firewall Management Center Virtual instances, 64 GB for the Firewall Management Center Virtual 300 (FMCv300). To improve performance, you can always increase a virtual appliance's memory and number of CPUs, depending on your available resources.

As a result of this memory check, we will not be able to support lower memory instances on supported platforms.

Memory and Resource Requirements

You can deploy the Firewall Management Center Virtual using VMware vSphere provisioning hosted on VMware ESX and ESXi hypervisors. See the Cisco Secure Firewall Threat Defense Compatibility Guide for hypervisor compatibility.

Important When upgrading the Firewall Management Center Virtual, check the latest Release Notes for details on whether a new release affects your environment. You may be required to increase resources to deploy the latest version.

When you upgrade, you add the latest features and fixes that help improve the security capabilities and performance of your deployment.

The specific hardware used for Firewall Management Center Virtual deployments can vary, depending on the number of instances deployed and usage requirements. Each virtual appliance you create requires a minimum resource allocation—memory, number of CPUs, and disk space—on the host machine.

We strongly recommend that you reserve CPU and memory resources to match the resource allocation. Failure to do so may significantly impact the Firewall Management Center Virtual performance and stability.

The following table lists the recommended and default settings for the Firewall Management Center Virtual appliance.

Important Be sure to allocate enough memory to ensure the optimal performance of your Firewall Management Center Virtual. If your Firewall Management Center Virtual has less than 32 GB memory, your system could experience policy deployment issues. To improve performance, you can increase a virtual appliance's memory and number of CPUs, depending on your available resources. Do not decrease the default settings, as they are the minimum required to run the system software.

Table 2: Firewall Management Center Virtual Appliance Settings

Setting	Minimum	Default	Recommended	Adjustable Setting?
Memory	28 GB	32 GB	32 GB	With restrictions. **Important** The Firewall Management Center Virtual platform has introduced a new memory check during upgrade. The Firewall Management Center Virtual upgrades to Version 6.6.0+ will fail if you allocate less than 28 GB RAM to the virtual appliance.
Virtual CPUs	4	4	16	Yes, up to 16
Hard disk provisioned size	250 GB	250 GB	n/a	No

Table 3: Firewall Management Center Virtual 300 (FMCv300) Virtual Appliance Settings

Setting	Default	Adjustable Setting?
Memory	64 GB	Yes
Virtual CPUs	32	No
Hard disk provisioned size	2.2 TB	No

Note Firewall Management Center Virtual 10.0 supports deployment on VMware vSphere / ESXi 8.0 platforms.

Insufficient allocation of RAM causes restart of processes due to Out Of Memory (OOM) events. Restarting database processes could also cause database corruption. In such cases, ensure that you upgrade the RAM to the required allocation and back up the database frequently to avoid any disruption due to database corruption.

Systems running VMware vCenter Server and ESXi instances must meet specific hardware and operating system requirements. For a list of supported platforms, see the VMware online Compatibility Guide.

Support for Virtualization Technology

The computer that serves as the ESXi host must meet the following requirements:

- It must have a 64-bit CPU that provides virtualization support, either Intel® Virtualization Technology (VT) or AMD Virtualization™ (AMD-V™) technology.
- Virtualization must be enabled in the BIOS settings

Note Both Intel and AMD provide online processor identification utilities to help you identify CPUs and determine their capabilities. Many servers that include CPUs with VT support might have VT disabled by default, so you must enable VT manually. You should consult your manufacturer's documentation for instructions on how to enable VT support on your system.

- If your CPUs support VT, but you do not see this option in the BIOS, contact your vendor to request a BIOS version that lets you enable VT support.
- To host virtual devices, the computer must have network interfaces compatible with Intel e1000 drivers (such as PRO 1000MT dual port server adapters or PRO 1000GT desktop adapters).

Verify CPU Support

You can use the Linux command line to get information about the CPU hardware. For example, the **/proc/cpuinfo** file contains details about individual CPU cores. Output its contents with **less** or **cat**.

You can look at the flags section for the following values:

- vmx—Intel VT extensions
- svm—AMD-V extensions

Use **grep** to quickly see if any of these values exist in the file by running the following command:

```
egrep "vmx|svm" /proc/cpuinfo
```

If your system supports VT, then you should see *vmx* or *svm* in the list of flags.

Guidelines and Limitations

OVF File Guidelines

Virtual appliances use Open Virtual Format (OVF) packaging. You deploy a virtual appliance with a virtual infrastructure (VI) or ESXi OVF template. The selection of the OVF file is based on the deployment target:

- For deployment on vCenter —Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-**VI**-*X.X.X-xxx*.ovf
- For deployment on ESXi(no vCenter)—Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-**ESXi**-*X.X.X-xxx*.ovf

where *X.X.X-xxx* is the version and build number of the System software you want to deploy. See

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

Note You must manage this virtual appliance using VMware vCenter.

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

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

Table 4: VMware OFV Template Settings

Setting	ESXi or VI	Action
Import/Deploy OVF Template	Both	Browse to the OVF templates you downloaded from Cisco.com.
OVF Template Details	Both	Confirm the appliance you are installing (Firewall Management Center 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	Select a datastore to store all files associated with the virtual machine.
Disk Format	Both	Select the format to store the virtual disks: thick provision lazy zeroed or thick provision eager zeroed. **Note** We recommend using the thick provisioned disk format to ensure optimal performance.
Network Mapping	Both	Select the management interface for the virtual appliance.
Properties	VI only	Customize the Virtual Machine initial configuration setup.

Time and Time Synchronization

Use a Network Time Protocol (NTP) server to synchronize system time on the Firewall Management Center Virtual and managed devices. You typically specify NTP servers during the Firewall Management Center Virtual initial configuration; see Firewall Management Center Virtual Initial Setup for the information about the default NTP servers.

Synchronizing the system time on your Firewall Management Center Virtual and its managed devices is essential to successful operation of your System. You can take additional steps to ensure time synchronization when you configure NTP on the VMware ESXi server to match the NTP settings of the Firewall Management Center Virtual.

You can use the vSphere Client to configure NTP on ESXi hosts. Consult VMware documentation for specific instructions. Additionaly, the VMware KB 2012069 describes how to configuring NTP on ESX/ESXi hosts using the vSphere Client.

vMotion Support

We recommend that you only use shared storage if you plan to use vMotion. During deployment, if you have a host cluster you can either provision storage locally (on a specific host) or on a shared host. However, if you try to vMotion the Firewall Management Center Virtual to another host, using local storage will produce an error.

Snapshots Support

A VMware snapshot is a copy of the virtual machine's disk file (VMDK) at a given point in time. Snapshots provide a change log for the virtual disk and can be used to restore a VM to a particular point in time when a failure or system error occurs. Snapshots alone do not provide backup, and should not be used as backup.

If you need configuration backups, use the backup and restore feature of the Firewall Management Center (**System** > **Tools** > **Backup/Restore**).

The VMware snapshots functionality on ESXi can exhaust VM storage capacity and impact the performance of the FMC virtual appliance. See the following VMware Knowledge Base articles:

- Best practices for using snapshots in the vSphere environment (VMware KB 1025279).
- Understanding VM snapshots in ESXi (VMware KB 1015180).

High Availability (HA) Support

You can establish high availability (HA) between two Firewall Management Center Virtual appliances on VMware ESXi.

- The two Firewall Management Center Virtual virtual appliances in a high availability configuration must be the same model.
- To establish the Firewall Management Center Virtual HA, Firewall Management Center Virtual requires an extra Firewall Management Center Virtual license entitlement for each Secure Firewall Threat Defense (formerly Firepower Threat Defense) device that it manages in the HA configuration. However, the required Firewall Threat Defense feature license entitlement for each Firewall Threat Defense device has no change regardless of the Firewall Management Center Virtual HA configuration. See *License Requirements for Threat Defense Devices in a High Availability Pair* in the Cisco Secure Firewall Management Center Device Configuration Guide for guidelines about licensing.

- If you break the Firewall Management Center Virtual HA pair, the extra Firewall Management Center Virtual license entitlement is released, and you need only one entitlement for each Firewall Threat Defense device.

See *Establishing Management Center High Availability* in the Cisco Secure Firewall Management Center Administration Guide for guidelines about high availability.

INIT Respawning Error Messages Symptom

You may see the following error message on the Firewall Management Center Virtual console running on ESXi 6 and ESXi 6.5:

```
"INIT: Id "fmcv" respawning too fast: disabled for 5 minutes"
```

Workaround—Edit the virtual machine settings in vSphere to add a serial port while the device is powered off.

1. Right-click the virtual machine and select **Edit Settings**.
2. On the Virtual Hardware tab, select **Serial port** from the **New device** drop-down menu, and click **Add**.

   The serial port appears at the bottom of the virtual device list.
3. On the **Virtual Hardware** tab, expand **Serial port**, and select connection type **Use physical serial port**.
4. Uncheck the **Connect at power on** checkbox.

   Click **OK** to save settings.

Limitations

The following limitations exist when deploying for VMware:

- Firewall Management Center Virtual appliances do not have serial numbers. The **System** > **Configuration** page will show either **None** or **Not Specified** depending on the virtual platform.
- Cloning a virtual machine is not supported.
- Restoring a virtual machine with snapshot is not supported.
- VMware Workstation, Player, Server, and Fusion do not recognize OVF packaging and are not supported.

Configure VMXNET3 Interfaces

Important

- From the 6.4 release, if you are using e1000 interfaces, we **strongly recommend** you switch to VMXNET3 interfaces. The VMXNET3 device drivers and network processing are integrated with the ESXi hypervisor, so they use fewer resources and offer better network performance.
- On 7.4 and earlier releases, FMCv300 supports e1000 interfaces only.

  From the 7.6 release, the FMCv300 supports both e1000 and VMXNET3 interfaces. By default, the management center virtual on VMware defaults to e1000 interfaces when you deploy the VM. We strongly recommend you switch to VMXNET3 interfaces.
- From the 10.0.0 release, the threat defense virtual and the management center virtual on VMware default to VMXNET3 interfaces when you deploy the VM.

To change e1000 interfaces to vmxnet3, you must delete ALL interfaces and reinstall them with the vmxnet3 driver.

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

Procedure

Step 1 Power off the Firewall Threat Defense Virtual or the Firewall Management Center Virtual Machine.

To change the interfaces, you must power down the appliance.

Step 2 Right-click the Firewall Threat Defense Virtual or the Firewall Management Center Virtual Machine in the inventory and select **Edit Settings**.

Step 3 Select the applicable network adapters and then select **Remove**.

Step 4 Click **Add** to open the **Add Hardware Wizard**.

Step 5 Select **Ethernet adapter** and click **Next**.

Step 6 Select the vmxnet3 adapter and then choose network label.

Step 7 Repeat for all interfaces on the Firewall Threat Defense Virtual.

What to do next

- Power on the Firewall Threat Defense Virtual or the Firewall Management Center Virtual from the VMware console.

Download the Installation Package

Cisco provides packaged virtual appliances for VMware ESX and 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. Each archive contains the OVF templates and manifest files for either an ESXi or VI deployment target, and a virtual machine disk format (vmdk) file.

Download the Firewall Management Center Virtual installation package from Cisco.com, and save it to your local disk. 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, 6.1 or 6.2).

Before you begin

Validate the SHA1 checksum after extracting the VMDK files from the directory.

Procedure

Step 1 Navigate to the Cisco Software Download page.

Note
A Cisco.com login and Cisco service contract are required.

Step 2 Click **Browse all** to search for the Firewall Management Center Virtual deployment package.

Step 3 Choose **Security** > **Firewalls** > **Firewall Management**, and select **Secure Firewall Management Center Virtual**.

Step 4 Find the VMware installation package that you want to download for the Firewall Management Center Virtual Appliance using the following naming convention:

Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-X.X.X-xxx.tar.gz

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

Step 5 Click the installation package you want to download.

Note
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 the Firewall Management Center Virtual, you should also download any new intrusion rule and Vulnerability Database (VDB) updates.

Step 6 Copy the installation package to a location accessible to the workstation or server that is running the vSphere Client.

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

Step 7 Uncompress the installation package archive file using your preferred tool and extract the installation files. For the Firewall Management Center Virtual:

- Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-X.X.X-xxx-disk1.vmdk
- Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-ESXi-X.X.X-xxx.ovf
- Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-ESXi-X.X.X-xxx.mf
- Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-VI-X.X.X-xxx.ovf
- Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-VI-X.X.X-xxx.mf

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

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

What to do next

- Determine your deployment target (VI or ESXi) and continue with Deploy the Firewall Management Center Virtual, on page 11.

Deploy the Firewall Management Center Virtual

You can use the VMware vSphere vCenter, vSphere Client, vSphere Web Client, or the ESXi hypervisor (for standalone ESXi deployment) to deploy the Firewall Management Center Virtual. You can deploy with either a VI 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 ESXi host. In either case, you must configure 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.

Procedure

Step 1 From the vSphere Client, choose **File** > **Deploy OVF Template**.

Step 2 From the drop-down list, select the OVF template you want to use to deploy your Firewall Management Center Virtual:

- Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-VI-*X.X.X-xxx*.ovf
- Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-ESXi-*X.X.X-xxx*.ovf
- Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-X.X.X-xxx-disk1.vmdk

where *X.X.X-xxx* is the version and build number of the installation package you downloaded from Cisco.com.

Step 3 View the **OVF Template Details** page and click **Next**.

Step 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 license and click **Next**.

Step 5 (Optional) Edit the name and select the folder location within the inventory where the Firewall Management Center 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.

Step 6 Select the host or cluster on which you want to deploy theFirewall Management Center Virtual and click Next.

Step 7 Navigate to, and select the resource pool where you want to run the Firewall Management Center Virtual and click **Next**.

This page appears only if the cluster contains a resource pool.

Step 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.

Step 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.

Note
We recommend using the Thick Provisioned disk format to ensure optimal performance.

Step 10 Associate the Firewall Management Center Virtual management interface with a VMware network on the Network Mapping screen.

Select a network by right-clicking the **Destination Networks** column in your infrastructure to set up the network mapping and click **Next**.

Step 11 If user-configurable properties are packaged with the OVF template (VI templates only), set the configurable properties and click **Next**.

Step 12 Review and verify the settings on the **Ready to Complete** window.

Step 13 (Optional) Check the **Power on after deployment** option to power on the Firewall Management Center Virtual, then click **Finish**.

Note: If you choose not to power on after deployment, you can do so later from the VMware console; see Initializing a Virtual Appliance.

Step 14 After the installation is complete, close the status window.

Step 15 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 Firewall Management Center Virtual instance then appears under the specified data center in the Inventory. Booting up the new VM could take up to 30 minutes.

Depending on the OVF template used, an ISO image **_ovfenv-<hostname>.iso** is mounted on the VMware vSphere vCenter, vSphere Client, vSphere Web Client, or the ESXi hypervisor (for standalone ESXi deployment) after the Firewall Management Center Virtual is deployed. This ISO image has OVF environment variables such as IP address netmask, hostnames, HA Roles, and so on. These variables are generated by vSphere and are used during the boot process.

You can also unmount the image after the Firewall Management Center Virtual VM has booted. However, the image will be mounted every time the Firewall Management Center Virtual is powered on or off, even if **Connect at power on** in the VMware vSphere **Network Adapter Configuration** is unchecked.

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

What to do next

- Confirm that the virtual appliance's hardware and memory settings meet the requirements for your deployment; see Verify the Virtual Machine Properties, on page 13.

Verify the Virtual Machine Properties

Use the VMware Virtual Machine Properties dialog box to adjust the host resource allocation for the selected virtual machine. You can change 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

Step 1 Right-click the name of your new virtual appliance, then choose **Edit Settings** from the context menu, or click **Edit virtual machine settings** from the **Getting Started** tab in the main window.

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

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:

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 Firewall Management Center Virtual, 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.

Step 5 Click **OK**.

What to do next

- Initialize the virtual appliance; see Power On and Initialize the Virtual Appliance, on page 14.
- Optionally, before you power on the appliance, you can create an additional management interface; see the *Deploy the Management Center Virtual Using VMware chapter of Cisco Secure Firewall Management Center Virtual Getting Started Guide* for more information.

Power On and Initialize the Virtual Appliance

After you complete the deployment of the 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 start over.

Procedure

Step 1 Power on the appliance.

In the vSphere Client, right-click the name of your virtual appliance from the inventory list, then select **Power** > **Power On** from the context menu.

Step 2 Monitor the initialization on the VMware console tab.

What to do next

After you deploy the Firewall Management Center Virtual, you must complete a setup process to configure the new appliance to communicate on your trusted management network. If you deploy with an ESXi OVF template on VMware, setting up the Firewall Management Center Virtual is a two-step process.

- To complete the initial setup of the Firewall Management Center Virtual, see Firewall Management Center Virtual Initial Setup.
- For an overview of the next steps needed in your Firewall Management Center Virtual deployment, see x`.