

Deploy the Firewall Management Center Virtual on Cisco Hyperflex

Cisco HyperFlex systems deliver hyperconvergence for any application, and anywhere. HyperFlex with Cisco Unified Computing System (Cisco UCS) technology that is managed through the Cisco Intersight cloud operations platform can power applications and data anywhere, optimize operations from a core datacenter to the edge and into public clouds, and therefore increase agility through accelerating DevOps practices.

You can deploy the Firewall Management Center Virtual on Cisco Hyperflex.

- Deploy the Firewall Management Center Virtual on Cisco Hyperflex, on page 1
- Deploy the Firewall Management Center Virtual, on page 4
- Power On and Initialize the Virtual Appliance, on page 5

Deploy the Firewall Management Center Virtual on Cisco Hyperflex

Cisco HyperFlex systems deliver hyperconvergence for any application, and anywhere. HyperFlex with Cisco Unified Computing System (Cisco UCS) technology that is managed through the Cisco Intersight cloud operations platform can power applications and data anywhere, optimize operations from a core datacenter to the edge and into public clouds, and therefore increase agility through accelerating DevOps practices.

You can deploy the Firewall Management Center Virtual on Cisco Hyperflex.

System Requirements

Firewall Management Center Virtual Requires 28 GB RAM

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

Memory and Resource Requirements

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

- For 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.
- The specific hardware used for the 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.
- 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. Do not decrease the default settings, as they are the minimum required to run the system software.

Table 1: Firewall Management Center Virtual Virtual Appliance Settings

Setting	Minimum	Default	Recommended	Adjustable Setting?
Memory	28 GB	32 GB	32 GB	With restrictions.
Virtual CPUs	4	4	8	Yes, up to 8
Hard disk provisioned size	250 GB	250 GB	n/a	No, based on Disk Format selection

Table 2: Firewall Management Center Virtual300 Virtual Appliance Settings

Setting	Default	Adjustable Setting?
Memory	64 GB	Yes
Virtual CPUs	32	No
Hard disk provisioned size	2.2 TB	No, based on Disk Format selection

For a list of supported platforms and specific hardware and operating system requirements, see the Compatibility Guide.

Guidelines and Limitations

Limitations

The following limitations exist when you deploy the Firewall Management Center Virtual for Cisco HyperFlex:

- The Firewall Management Center Virtual appliances do not have serial numbers. The **System** > **Configuration** page shows 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.

OVF File Guidelines

Virtual appliances use Open Virtual Format (OVF) packaging. You deploy a virtual appliance with a virtual infrastructure (VI) 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

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

High Availability Support

You can establish high availability (HA) between two Firewall Management Center Virtual appliances deployed on Hyperflex host:

- The two Firewall Management Center 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 the Firewall Threat Defense device that it manages in the HA configuration. However, the required Firewall Threat Defense feature license entitlement for each the 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 the Firewall Threat Defense device.

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

Related Documents

Release Notes for Cisco HX Data Platform

Configuration Guides for Cisco HX Data Platform

Cisco HyperFlex 4.0 for Virtual Server Infrastructure with VMware ESXi

Cisco HyperFlex Systems Solutions Overview

Cisco HyperFlex Systems Documentation Roadmap

Deploy the Firewall Management Center Virtual

Use this procedure to deploy the Firewall Management Center Virtual appliance to Cisco Hyperflex on a vSphere vCenter Server.

Before you begin

- Ensure that you have deployed Cisco HyperFlex and performed all the post-installation configuration tasks. For more information, see Cisco HyperFlex Systems Documentation Roadmap.
- You must have at least one network configured in vSphere (for management) before you deploy the Firewall Management Center Virtual.
- Download the Firewall Management Center Virtual VI OVF template file from Cisco.com: *Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-VI-X.X.X-xxx.ovf*, where *X.X.X-xxx* is the version and build number.

Procedure

Step 1 Log in to the vSphere Web Client.

Step 2 Select the Hyperflex cluster where you want to deploy the Firewall Management Center Virtual, and click **ACTIONS** > **Deploy OVF Template**.

Step 3 Browse your file system for the OVF template source location, and click **NEXT**

You want to select the Firewall Management Center Virtual VI OVF template:

Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-VI-X.X.X-xxx.ovf

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

Step 4 Specify a name and folder for the Firewall Management Center Virtual deployment, and click **NEXT**.

Step 5 Select a compute resource, and wait until the compatibility check is complete. If the compatibility check succeeds, click **NEXT**.

Step 6 Review the OVF template information (product name, vendor, version, download size, size on disk, and description), and click **NEXT**.

Step 7 Review and accept the license agreement that is packaged with the OVF template (VI templates only), and click **NEXT**.

Step 8 Select a storage location and virtual disk format, and click **NEXT**.

On this window, you select from datastores already configured on the destination HyperFlex cluster. 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.

When you select **Thick Provisioned** as the virtual disk format, all storage is immediately allocated. When you select **Thin Provisioned** as the virtual disk format, 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.

Step 9 Map the networks specified in the OVF template to networks in your inventory, and click **NEXT**.

Step 10 Set the user-configurable properties packaged with the OVF template:

Note You must mandatorily configure all the required customizations in this step.

a) **Password**

Set the password for the Firewall Management Center Virtual admin access.

b) **Network**

Set the network information, including the Fully Qualified Domain Name (FQDN), DNS, and network protocol (IPv4 or IPv6).

c) Click **NEXT**.

Step 11 Review and verify the displayed information. To begin the deployment with these settings, click **FINISH**. To make any changes, click **BACK** to navigate back through the screens.

After you complete the wizard, the vSphere Web Client processes the virtual machine; 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 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 Firewall Management Center Virtual with the Cisco Licensing Authority, the Firewall Management Center requires Internet access. You need to perform additional configuration after deployment to achieve Internet access and successful license registration. DNS server configuration is mandatory for license registration.

What to do next

Initialize the virtual appliance; see Power On and Initialize the Virtual Appliance

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 VM console.

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 a VI OVF template on Hyperflex, 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 Cisco Secure Firewall Management Center Virtual Getting Started Guide.