Introduction to the Cisco Firepower Management Center Virtual Appliance

The Cisco Firepower Management Center Virtual Appliance (FMCv) brings full firewall functionality to virtualized environments to secure data center traffic and multi-tenant environments. Firepower Management Center Virtual can manage physical and virtual Firepower Threat Defense, Firepower NGIPS, and FirePOWER appliances.

Platforms and Support for the FMCv

Memory and Resource Requirements

Each instance of the FMCv requires a minimum resource allocation—memory, number of CPUs, and disk space—on the target platform to ensure optimal performance.

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

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

FMCv Requires 28 GB RAM for Upgrade (6.6.0+)

The FMCv platform has introduced a new memory check during upgrade. FMCv 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 FMCv instances, 64 GB for the FMCv 300. 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. See About Virtual Appliance Performance, on page 3 for important FMCv upgrade information.

FMCv Initial Setup (6.5.0+)

Beginning with Version 6.5, the FMCv has an improved initial setup experience that includes the following changes and enhancements:

- **DHCP on Management**—DHCP is enabled by default mode on the management interface (eth0).

  The FMCv management interface is preconfigured to accept an IP4 address assigned by DHCP. Consult with your system administrator to determine what IP address your DHCP has been configured to assign to the FMCv. In scenarios where no DHCP is available, the FMC management interface uses the IPv4 address 192.168.45.45.

- **Web interface URL**—The default URL for the FMCv web interface has changed to *https://<FMC-IP>:<port>/ui/login*.

- **Password reset**—To ensure system security and privacy, the first time you log in to the FMC you are required to change the **admin** password. When the Change Password wizard screen appears, you have two options: Enter a new password in the **New Password** and **Confirm Password** text boxes. The password must comply with the criteria listed in the dialog.

- **Network settings**—The FMCv now includes an install wizard to complete the initial setup:

  - **Fully Qualified Domain Name**—Accept the default value, if one is shown, or enter a fully qualified domain name (syntax <hostname>.<domain>) or host name.

  - **Boot protocol for IPV4 connection**—Choose either DHCP or Static/Manual as the method of IP address assignment.

  - **DNS Group**—The default Domain Name Server group for the FMCv is the Cisco Umbrella DNS.

  - **NTP Group Servers**—The default Network Time Protocol group is set to the Sourcefire NTP pools.

- **RAM Requirements**—The recommended size of RAM is 32GB for the FMCv.

- **FMCv-300 for VMware**—A new scaled FMCv image is available on the VMware platform that supports managing up to 300 devices and has higher disk capacity.

Supported Platforms

The Cisco Firepower Management Center Virtual can be deployed on the following platforms:

- **VMware vSphere Hypervisor (ESXi)**—You can deploy the Firepower Management Center Virtual as a guest virtual machine on VMware ESXi.

- **Kernel Virtualization Module (KVM)**—You can deploy the Firepower Management Center Virtual on a Linux server that is running the KVM hypervisor.

- **Amazon Web Services (AWS)**—You can deploy the Firepower Management Center Virtual on EC2 instances in the AWS Cloud.

- **Microsoft Azure**—You can deploy the Firepower Management Center Virtual in the Azure Cloud.

Note High availability (HA) configuration is supported only on the Firepower Management Center Virtual deployment on VMWare; see *About Firepower Management Center High Availability* in the Firepower Management Center Configuration Guide for information about system requirements for high availability.

Hypervisor and Version Support

For hypervisor and version support, see Cisco Firepower Compatibility.

Firepower Management Center Virtual Licenses

The Firepower Management Center Virtual License is a platform license, rather than a feature license. The version of virtual license you purchase determines the number of devices you can manage via the Firepower Management Center. For example, you can purchase licenses that enable you to manage two devices, 10 devices, 25 devices, or 300 devices.

About Firepower Feature Licenses

You can license a variety of features to create an optimal Firepower System deployment for your organization. The Firepower Management Center allows you to manage these feature licenses and assign them to your devices.

Note The Firepower Management Center manages feature licenses for your devices, but you do not need a feature license to use a Firepower Management Center.

Firepower feature licenses depend on your device type:

- Smart Licenses are available for Firepower Threat Defense and Firepower Threat Defense Virtual devices.
- Classic Licenses are available for 7000 and 8000 Series, ASA FirePOWER, and NGIPSv devices.

Devices that use Classic Licenses are sometimes referred to as Classic devices. A single Firepower Management Center can manage both Classic and Smart Licenses.

In addition to "right-to-use" feature licenses, many features require a service subscription. Right-to-use licenses do not expire, but service subscriptions require periodic renewal.

For detailed information about Smart vs. Classic licenses on each platform, see the Cisco Firepower System Feature Licenses document.

For answers to common questions about Smart Licensing, Classic licensing, right-to-use licenses, and service subscriptions, see the Frequently Asked Questions (FAQ) about Firepower Licensing document.

About Virtual Appliance Performance

It is not possible to accurately predict throughput and processing capacity for virtual appliances. A number of factors heavily influence performance, such as the:

- Amount of memory and CPU capacity of the host
- Number of total virtual machines running on the host
- Network performance, interface speed, and number of sensing interfaces deployed
- Amount of resources assigned to each virtual appliance
- Level of activity of other virtual appliances sharing the host
- Complexity of policies applied to a virtual device

If the throughput is not satisfactory, adjust the resources assigned to the virtual appliances that share the host.

Each virtual appliance you create requires a certain amount of memory, CPUs, and hard disk space on the host. 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.

FMCv Default and Minimum Memory Requirements

All FMCv implementations now have the same RAM requirements: 32 GB recommended, 28 GB required (64 GB for FMCv 300). Upgrades to Version 6.6.0+ will fail if you allocate less than 28 GB to the virtual appliance. After upgrade, the health monitor will alert if you lower the memory allocation.

These new memory requirements enforce uniform requirements across all virtual environments, improve performance, and allow you to take advantage of new features and functionality. We recommend you do not decrease the default settings. To improve performance, you can increase a virtual appliance's memory and number of CPUs, depending on your available resources.

Important As of the Version 6.6.0 release, lower-memory instance types for cloud-based FMCv deployments (AWS, Azure) are fully deprecated. You cannot create new FMCv instances using them, even for earlier Firepower versions. You can continue running existing instances.

The following table summarizes pre-upgrade requirements for lower-memory FMCv deployments.

Table 1: FMCv Memory Requirements for Version 6.6.0+ Upgrades

Platform	Pre-Upgrade Action	Details
VMware	Allocate 28 GB minimum/32 GB recommended.	Power off the virtual machine first. For instructions, see the VMware documentation.
KVM	Allocate 28 GB minimum/32 GB recommended.	For instructions, see the documentation for your KVM environment.

Platform	Pre-Upgrade Action	Details
AWS	Resize instances: • **From** c3.xlarge **to** c3.4xlarge. • **From** c3.2.xlarge **to** c3.4xlarge. • **From** c4.xlarge **to** c4.4xlarge. • **From** c4.2xlarge **to** c4.4xlarge. We also offer a c5.4xlarge instance for new deployments.	Stop the instance before you resize. Note that when you do this, data on the instance store volume is lost, so migrate your instance store-backed instance first. Additionally, if your management interface does not have an Elastic IP address, its public IP address is released. For instructions, see the documentation on changing your instance type in the AWS user guide for Linux instances.
Azure	Resize instances: • **From** Standard_D3_v2 **to** Standard_D4_v2.	Use the Azure portal or PowerShell. You do not need to stop the instance before you resize, but stopping may reveal additional sizes. Resizing restarts a running virtual machine. For instructions, see the Azure documentation on resizing a Windows VM.

Download the Firepower Management Center Virtual Deployment Package

You can download Firepower Management Center Virtual deployment packages from Cisco.com, or in the case of patches and hotfixes, you can download from within the Firepower Management Center.

To download the Firepower Management Center Virtual deployment package:

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 Firepower Management Center Virtualdeployment package.

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

Step 4 Choose your *model* > **FireSIGHT System Software** > *version*.

The following table includes naming conventions and information about Firepower Management Center Virtual software on Cisco.com.

Model	Package Type	Package Name
Firepower Management Center Virtual	Firepower software install: VMware	Cisco_Firepower_Management_Center_Virtual_VMware-*version*.**tar.gz**
	Firepower software install: KVM	Cisco_Firepower_Management_Center_Virtual-*version*.**qcow2**
	Firepower software install: AWS	Log into the cloud service and deploy from the marketplace.
	Firepower software install: Azure	Log into the cloud service and deploy from the marketplace.

Step 5 Locate the deployment package and download it to a server or to your management computer.

Many package names look similar, so make sure you download the correct one.

Download directly from the Cisco Support & Download site. If you transfer a deployment package by email, it may become corrupted.

What to do next

Refer to the chapter that is applicable for your deployment platform:

- To deploy the Firepower Management Center Virtual as a guest virtual machine on VMware ESXi, see Deploy the Firepower Management Center Virtual Using VMware.
- To deploy the Firepower Management Center Virtual on a Linux server running the KVM hypervisor, see Deploy the Firepower Management Center Virtual Using KVM.
- To deploy the Firepower Management Center Virtual in AWS, see Deploy the Firepower Management Center Virtual On the AWS Cloud.
- To deploy the Firepower Management Center Virtual in Azure, see Deploy the Firepower Management Center Virtual On the Microsoft Azure Cloud.