Introduction to the Secure Firewall Management Center Virtual Appliance

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

Platforms and Support for the Firewall Management Center Virtual

Memory and Resource Requirements

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

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 versions.

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

Firewall Management Center Virtual Requires 32 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 32 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. See About Virtual Appliance Performance, on page 4 for important Firewall Management Center Virtual upgrade information.

Firewall Management Center Virtual Initial Setup (6.5.0+)

Beginning with Version 6.5, the Firewall Management Center Virtual 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 Firewall Management Center Virtual management interface is preconfigured to accept an IP4 or IPv6 address assigned by DHCP. Consult with your system administrator to determine what IP address your DHCP has been configured to assign to the Firewall Management Center Virtual. In scenarios where no DHCP is available, the Secure Firewall Management Center (formerly Firepower Management Center) management interface uses the IPv4 address 192.168.45.45 or the IPv6 address, for example: 2001:db8::a111:b221:1:abca/96.

Note If you use DHCP, you must use DHCP reservation, so the assigned address does not change. If the DHCP address changes, device registration will fail because the Firewall Management Center network configuration gets out of sync. To recover from a DHCP address change, connect to the Firewall Management Center (using the hostname or the new IP address) and navigate to **System** > **Configuration** > **Management Interfaces** to reset the network.

- **Web interface URL**—The default URL for the Firewall Management Center Virtual web interface has changed to *https://<-IP>:<port>/ui/login*.
- **Password reset**—To ensure system security and privacy, the first time you log in to the Firewall Management Center 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 Firewall Management Center Virtual 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 or IPV6connection**—Choose either DHCP or Static/Manual as the method of IP address assignment.
  - **DNS Group**—The default Domain Name Server group for the Firewall Management Center Virtual 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 Firewall Management Center Virtual.
- **FMCv300 for VMware**—A new scaled Firewall Management Center Virtual image is available on the VMware platform that supports managing up to 300 devices and has higher disk capacity.

Supported Platforms

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

- **VMware vSphere Hypervisor (ESXi)** — You can deploy the Firewall Management Center Virtual as a guest virtual machine on VMware ESXi.
- **Kernel Virtualization Module (KVM)** — You can deploy the Firewall Management Center Virtual on a Linux server that is running the KVM hypervisor.
- **Amazon Web Services (AWS)** — You can deploy the Firewall Management Center Virtual on EC2 instances in the AWS Cloud.
- **Microsoft Azure** — You can deploy the Firewall Management Center Virtual in the Azure Cloud.
- **Google Cloud Platform (GCP)** — You can deploy the Firewall Management Center Virtual on the public GCP.
- **Oracle Cloud Infrastructure (OCI)** — You can deploy the Firewall Management Center Virtual on the OCI.
- **OpenStack** — You can deploy the Firewall Management Center Virtual on the OpenStack. This deployment uses a KVM hypervisor to manage virtual resources.
- **Cisco HyperFlex** — You can deploy the Firewall Management Center Virtual on the Cisco HyperFlex.
- **Nutanix** — You can deploy the Firewall Management Center Virtual on the Nutanix environment with AHV hypervisor.
- **Alibaba Cloud** — You can deploy the Firewall Management Center Virtual on the Alibaba Cloud.
- **Microsoft Hyper-V** — You can deploy the Firewall Management Center Virtual on Microsoft Hyper-V.

Note High availability (HA) configuration is supported on the Firewall Management Center Virtual deployment on VMware, AWS, Azure, KVM, OCI, and HyperFlex. See *High Availability* in the Management Center Administration Guide for information about system requirements for high availability.

Hypervisor and Version Support

For hypervisor and version support, see Secure Firewall Threat Defense Compatibility.

Firewall Management Center Virtual Licenses

The Firewall 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 Firewall Management Center. For example, you can purchase licenses that enable you to manage two devices, 10 devices, 25 devices, or 300 devices.

About Firewall Management Center Feature Licenses

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

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

Firewall Management Center feature licenses depend on your device type:

- Smart Licenses are available for the Firewall Threat Defense and Firewall 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 Firewall 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 licenses platform, see Licenses in the Secure Firewall Management Center Administration Guide.

For answers to common questions about Smart Licensing, Classic licensing, right-to-use licenses, and service subscriptions, see Secure Firewall Management Center Feature Licenses.

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.

The following table lists the supported Firewall Management Center Virtual limits.

Table 1: Supported Management Center Virtual Limits

Component	FMCv2/FMCv10/FMCv25	FMCv300
vCPU	8/4 vCPUs	32 vCPUs
Memory	32 GB	64 GB
Event storage space	250 GB	2.2 TB
Maximum network map size (hosts/users)	50,000/50,000	150,000/150,000
Maximum event rate (events per second)	5,000	12,000 eps

Firewall Management Center Virtual Default and Minimum Memory Requirements

All the Firewall Management Center Virtual implementations now have the same RAM requirements: 32 GB required (64 GB for the FMCv300). Upgrades to Version 6.6.0+ will fail if you allocate less than 32 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 Firewall Management Center Virtual deployments (AWS, Azure) are fully deprecated. You cannot create the new Firewall Management Center Virtual instances using them, even for earlier versions. You can continue running existing instances.

The following table summarizes pre-upgrade requirements for lower-memory Firewall Management Center Virtual deployments.

Table 2: Firewall Management Center Virtual Memory Requirements for Version 6.6.0+ Upgrades

Platform	Pre-Upgrade Action	Details
VMware	Allocate 32 GB minimum.	Power off the virtual machine first. For instructions, see the VMware documentation.
KVM	Allocate 32 GB minimum.	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.
GCP	Allocate memory based on the GCP instance type.	See GCP Machine Type Support for more information.
OCI	Allocate memory based on the OCI instance type.	See OCI Compute Shapes for more information.
OpenStack	Allocate 32 GB minimum.	See Memory and resource requirements for more information.
HyperFlex	Allocate 32 GB minimum.	See Host System Requirements for more information.
Nutanix	Allocate 32 GB minimum.	See Host System Requirements for more information.

Download the Firewall Management Center Virtual Deployment Package

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

To download the Firewall Management Center Virtual deployment package:

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

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

Model	Package Type	Package Name
Firewall Management Center Virtual	Software install: VMware	Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-*version*.**tar.gz**
	Software install: KVM	Cisco_Secure_FW_Mgmt_Center_Virtual_KVM-*version*.**qcow2**
	Software install: AWS	Log into the cloud service and deploy from the marketplace.
	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 Firewall Management Center Virtual as a guest virtual machine on VMware ESXi, see Deploy the Firewall Management Center Virtual on VMware.
- To deploy the Firewall Management Center Virtual on a Linux server running the KVM hypervisor, see Deploy the Firewall Management Center Virtual on KVM.
- To deploy the Firewall Management Center Virtual in AWS, see Deploy the Firewall Management Center Virtual on AWS.
- To deploy the Firewall Management Center Virtual in Azure, see Deploy the Firewall Management Center Virtual on Azure.
- To deploy the Firewall Management Center Virtual in Google Cloud Platform, see Deploy the Management Center Virtual On the Google Cloud Platform.
- To deploy the Firewall Management Center Virtual in Oracle Cloud Infrastructure, see Deploy the Management Center Virtual On the Oracle Cloud Infrastructure.
- To deploy the Firewall Management Center Virtual using OpenStack, see Deploy the Management Center Virtual Using OpenStack.
- To deploy the Firewall Management Center Virtual using Cisco Hyperflex, see Deploy the Management Center Virtual Using Cisco Hyperflex.

- To deploy the Firewall Management Center Virtual using Nutanix, see Deploy the Management Center Virtual Using Nutanix.
- To deploy the Firewall Management Center Virtual on Hyper-V, see Deploy the Firewall Management Center Virtual on Hyper-V.