

Cisco Secure Firewall Management Center Virtual Getting Started Guide

First Published: 2015-11-10

Last Modified: 2026-09-21

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2015–2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Introduction to the Firewall Management Center Virtual** 1

Platforms and Support for the Firewall Management Center Virtual 1

Firewall Management Center Virtual Licenses 4

About Firewall Management Center Feature Licenses 4

About Virtual Appliance Performance 4

Download the Firewall Management Center Virtual Deployment Package 6

CHAPTER 2 **Deploy the Firewall Management Center Virtual on VMware** 9

VMware Feature Support for the Firewall Management Center Virtual 9

System Requirements 10

Guidelines and Limitations 13

Configure VMXNET3 Interfaces 17

Download the Installation Package 17

Deploy the Firewall Management Center Virtual 19

Verify the Virtual Machine Properties 21

Power On and Initialize the Virtual Appliance 22

CHAPTER 3 **Deploy the Firewall Management Center Virtual on KVM** 23

Overview 23

Prerequisites 25

Guidelines and Limitations 26

Prepare the Day 0 Configuration File 27

Deploy the Firewall Management Center Virtual 28

Launch Using a Deployment Script 28

Deploy the Firewall Management Center Virtual 30

Deploy Without Using the Day 0 Configuration File 31

Configure Network Settings Using a Script 32
Perform Initial Setup Using the Web Interface 32

CHAPTER 4 Deploy the Firewall Management Center Virtual on AWS 35
Overview 35
AWS Solution Overview 37
Guidelines and Limitations 38
Configure the AWS Environment 39
Create the VPC 39
Add the Internet Gateway 40
Add Subnets 41
Add a Route Table 41
Create a Security Group 42
Create Network Interfaces 43
Create Elastic IPs 44
Deploy the Firewall Management Center Virtual 44

CHAPTER 5 Deploy the Firewall Management Center Virtual on Azure 49
Overview 49
Prerequisites 51
Guidelines and Limitations 51
Resources Created During Deployment 53
Deploy the Firewall Management Center Virtual 54
Deploy from Azure Marketplace Using the Solution Template 54
Deploy from Azure Using a VHD and Resource Template 58
Deploy the Azure Marketplace offers in the restricted Azure Private Marketplace environment 61
Deploy the IPv6 Supported on Azure 63
Deploy the IPv6 Supported Secure Firewall Management Center Virtual on Azure 63
About IPv6 Supported Deployment on Azure 63
Deploy from Azure using a Custom IPv6 Template with Marketplace Image References 64
Deploy from Azure Using a VHD and Custom IPv6 Template 69
Verify the Firewall Management Center Virtual Deployment 74
Monitoring and Troubleshooting 76
Feature History 77

CHAPTER 6 **Deploy the Firewall Management Center Virtual on GCP** 79

Overview 79

Prerequisites 80

Guidelines and Limitations 81

Sample Network Topology 81

Deploy the Firewall Management Center Virtual 82

Create VPC Networks 82

Create the Firewall Rules 83

Create the Firewall Management Center Virtual Instance on GCP 83

Access the Firewall Management Center Virtual Instance on GCP 85

Connect to the Firewall Management Center Virtual Instance Using the Serial Console 86

Connect to the Firewall Management Center Virtual Instance Using an External IP 86

Connect to the Firewall Management Center Virtual Instance Using Gcloud 86

CHAPTER 7 **Deploy the Firewall Management Center Virtual on OCI** 89

Overview 89

Prerequisites 91

Guidelines and Limitations 91

Sample Network Topology 91

Deploy the Firewall Management Center Virtual 92

Configure the Virtual Cloud Network (VCN) 92

Create the Network Security Group 93

Create the Internet Gateway 93

Create the Subnet 94

Create the Firewall Management Center Virtual Instance on OCI 95

Access the Firewall Management Center Virtual Instance on OCI 96

Connect to the Firewall Management Center Virtual Instance Using PuTTY 96

Connect to the Firewall Management Center Virtual Instance Using SSH 97

Connect to the Firewall Management Center Virtual Instance Using OpenSSH 98

CHAPTER 8 **Deploy the Firewall Management Center Virtual on OpenStack** 99

Overview 99

Prerequisites 99

Guidelines and Limitations 100
System Requirements 101
Sample Network Topology 102
Deploy the Firewall Management Center Virtual 103
Upload the Firewall Management Center Virtual Image to OpenStack 103
Create the Network Infrastructure for the OpenStack and the Firewall Management Center Virtual 104
Create the Firewall Management Center Virtual Instance on OpenStack 105

CHAPTER 9 **Deploy the Firewall Management Center Virtual on Cisco Hyperflex 107**
Deploy the Firewall Management Center Virtual on Cisco Hyperflex 107
System Requirements 107
Guidelines and Limitations 108
Deploy the Firewall Management Center Virtual 110
Power On and Initialize the Virtual Appliance 111

CHAPTER 10 **Deploy the Firewall Management Center Virtual on Nutanix 113**
Overview 113
System Requirements 113
Prerequisites 114
Guidelines and Limitations 115
Deploy the Firewall Management Center Virtual on Nutanix 116
Upload the Firewall Management Center Virtual QCOW2 File to Nutanix 116
Prepare the Day 0 Configuration File 117
Deploy the Firewall Management Center Virtual to Nutanix 118
Complete the Firewall Management Center Virtual Setup 120
Configure Network Settings Using a Script 121
Perform Initial Setup Using the Web Interface 122

CHAPTER 11 **Deploy the Firewall Management Center Virtual on Alibaba Cloud 123**
Overview 123
Guidelines and Limitations 124
Prerequisites 125
Deploy the Firewall Management Center Virtual 125

CHAPTER 12 **Deploy the Firewall Management Center Virtual on Hyper-V** 129

Overview 129

Sample Topology of Management Center Virtual on Hyper-V 130

Supported Windows Server for Management Center Virtual 130

Guidelines and Limitations for Management Center Virtual on Hyper-V 130

Licenses for Deployment of Management Center Virtual on Hyper-V 131

Prerequisites for Deployment of Management Center Virtual on Hyper-V 131

Deploy the Management Center Virtual 131

Download Management Center Virtual VHD Image 131

Prepare Day 0 Configuration File 132

Create a New Virtual Switch 133

Create a New Virtual Machine 133

Verify the Deployment 134

Access First Boot Logs 134

Shut Down Management Center Virtual 135

Reboot Management Center Virtual 135

Delete Management Center Virtual 135

Troubleshooting 136

CHAPTER 13 **Firewall Management Center Virtual Initial Setup** 137

Firewall Management Center Initial Setup Using the CLI for Versions 6.5 and Later 137

Perform Initial Setup at the Web Interface for Versions 6.5 and Later 140

Review Automatic Initial Configuration for Versions 6.5 and Later 144

CHAPTER 14 **Firewall Management Center Virtual Initial Administration and Configuration** 147

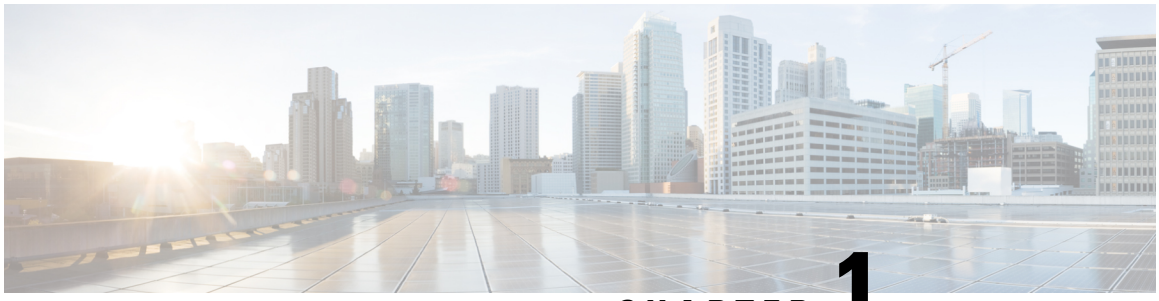
Individual User Accounts 147

Device Registration 148

Health and System Policies 148

Software and Database Updates 148

Troubleshooting 149



CHAPTER 1

Introduction to the Firewall Management Center Virtual

The Secure Firewall Management Center Virtual (formerly Firepower Management Center Virtual) brings full firewall functionality to virtualized environments to secure data center traffic and multi-tenant environments.

- Platforms and Support for the Firewall Management Center Virtual, on page 1
- Firewall Management Center Virtual Licenses, on page 4
- About Virtual Appliance Performance, on page 4
- Download the Firewall Management Center Virtual Deployment Package, on page 6

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



Note Devices registered to a Firewall Management Center Virtual for analytics-only purposes still count toward the Firewall Management Center Virtual platform device capacity limit.

Event processing requirements increase with the number of registered devices, regardless of whether they are fully managed or used only for analytics. Therefore, you must appropriately size your Firewall Management Center Virtual deployment when planning analytics-only use cases.

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.
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.

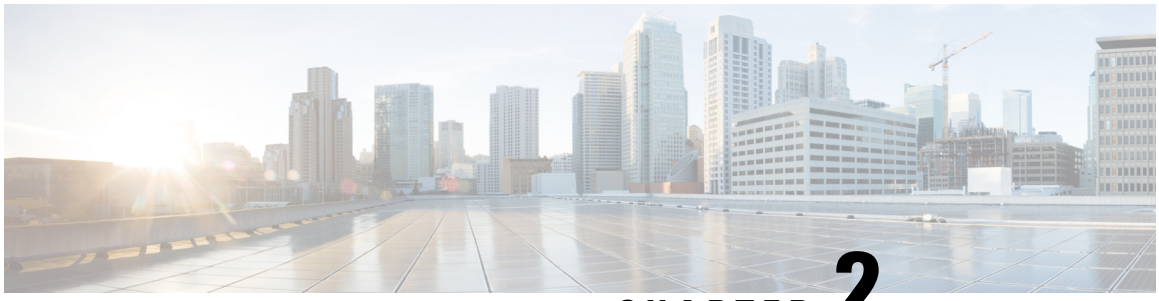
Download directly from the Cisco Support & Download site. If you transfer a deployment package by email, it may become corrupted.

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, on page 9.
- To deploy the Firewall Management Center Virtual on a Linux server running the KVM hypervisor, see Deploy the Firewall Management Center Virtual on KVM, on page 23.
- To deploy the Firewall Management Center Virtual in AWS, see Deploy the Firewall Management Center Virtual on AWS, on page 35.
- To deploy the Firewall Management Center Virtual in Azure, see Deploy the Firewall Management Center Virtual on Azure, on page 49.

- 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 Alibaba Cloud, see Deploy the Management Center Virtual On the Alibaba Cloud.
- To deploy the Firewall Management Center Virtual on Hyper-V, see Deploy the Firewall Management Center Virtual on Hyper-V, on page 129.



CHAPTER 2

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, on page 9
- System Requirements, on page 10
- Guidelines and Limitations, on page 13
- Download the Installation Package, on page 17
- Deploy the Firewall Management Center Virtual, on page 19
- Verify the Virtual Machine Properties, on page 21
- Power On and Initialize the Virtual Appliance, on page 22

VMware Feature Support for the Firewall Management Center Virtual

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

Table 3: 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 15 .
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 15.
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 4: 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 5: 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 ESXi version 8.0 is supported on Management Center Virtual 10.0.0 and later versions. ESXi versions 9.0 and 9.1 are supported on Management Center Virtual 10.1.0 and later versions.

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 6: 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, on page 137 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 19.

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 21.

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 22.
- 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.

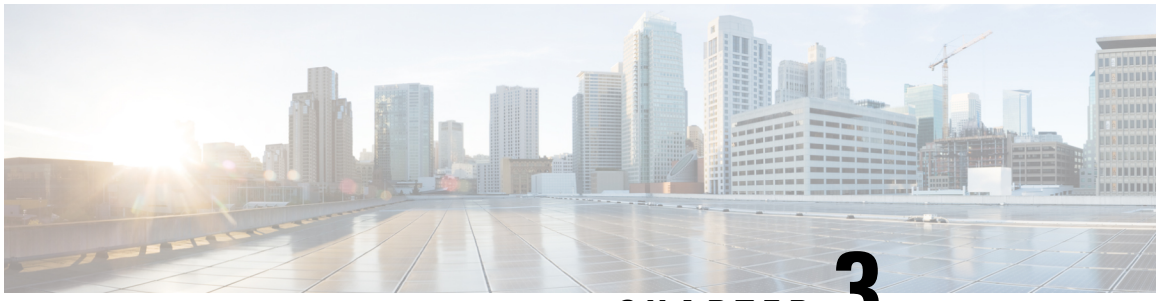
In the vSphere Client, right-click the name of your virtual appliance from the inventory list, then select **Power** > **Power On** from the context menu.

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, on page 137.
- For an overview of the next steps needed in your Firewall Management Center Virtual deployment, see Firewall Management Center Virtual Initial Administration and Configuration, on page 147.



CHAPTER 3

Deploy the Firewall Management Center Virtual on KVM

You can deploy the Firewall Management Center Virtual on KVM.

- Overview, on page 23
- Prerequisites, on page 25
- Guidelines and Limitations, on page 26
- Prepare the Day 0 Configuration File, on page 27
- Deploy the Firewall Management Center Virtual, on page 28
- Deploy Without Using the Day 0 Configuration File, on page 31

Overview

KVM is a full virtualization solution for Linux on x86 hardware containing virtualization extensions (such as Intel VT). It consists of a loadable kernel module, kvm.ko, that provides the core virtualization infrastructure and a processor specific module, such as kvm-intel.ko.

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 Firewall Management Center Virtual instances, 64 GB RAM 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 run multiple virtual machines running unmodified OS images using KVM. Each virtual machine has private virtualized hardware: a network card, disk, graphics adapter, and so forth. 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 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 lists the recommended and default settings for the Firewall Management Center Virtual appliance on KVM:

- Processors
  - Requires 4 vCPUs
- Memory
  - Minimum required 28 / Recommended (default) 32 GB RAM



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.

- Networking
  - Supports virtio drivers
  - Supports one management interface
  - IPv6
- Host storage per Virtual Machine
  - The Firewall Management Center Virtual requires 250 GB
  - Supports virtio and scsi block devices
- Console
  - Supports terminal server via telnet

Starting from version 7.3, Management Center Virtual 300 (FMCv300) is supported on KVM. The following lists the recommended and default settings for the FMCv300 appliance on KVM:

- Processors
  - Requires 32 vCPUs
- Memory
  - Recommended (default) 64 GB RAM
- Networking
  - Supports virtio drivers
  - Supports one management interface
- Host storage per Virtual Machine
  - The FMCv300 requires 2 TB
  - Supports virtio and scsi block devices
- Console
  - Supports terminal server via telnet

Prerequisites

- Download the Firewall Management Center Virtual qcow2 file from Cisco.com and put it on your Linux host:

  https://software.cisco.com/download/navigator.html
- A Cisco.com login and Cisco service contract are required.
- For the purpose of the sample deployment in this document, we assume you are using Ubuntu 24.04 LTS. Install the following packages on top of the Ubuntu 24.04 LTS host:
  - qemu-kvm
  - libvirt-daemon-system
  - bridge-utils
  - virt-manager
  - virtinst
  - libvirt-clients
  - genisoimage
- Performance is affected by the host and its configuration. You can maximize the throughput on KVM by tuning your host. For generic host-tuning concepts, see Network Function Virtualization: Quality of Service in Broadband Remote Access Servers with Linux and Intel Architecture.
- Useful optimizations for Ubuntu 24.04 LTS include the following:

- macvtap—High performance Linux bridge; you can use macvtap instead of a Linux bridge. Note that you must configure specific settings to use macvtap instead of the Linux bridge.
- Transparent Huge Pages—Increases memory page size and is on by default in Ubuntu 24.04.
- Hyperthread disabled—Reduces two vCPUs to one single core.
- txqueuelength—Increases the default txqueuelength to 4000 packets and reduces drop rate.
- pinning—Pins qemu and vhost processes to specific CPU cores; under certain conditions, pinning is a significant boost to performance.

- For information on optimizing a RHEL-based distribution, see Red Hat Enterprise Linux 9 Configuring and Managing Virtualization.

Guidelines and Limitations

- The 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.
- Nested hypervisors (KVM running on top of VMware/ESXi) are not supported. Only bare-metal KVM deployments are supported.
- Cloning a virtual machine is not supported.

High Availability support

- Management Center Virtual 300 (FMCv300) for KVM—A new scaled Firewall Management Center Virtual image is available for KVM that supports managing up to 300 devices and has higher disk capacity.
- Firewall Management Center Virtual High Availability (HA) is supported.
- 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 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 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 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 *High Availability* in the Secure Firewall Management Center Device Configuration Guide for more information and guidelines about high availability.

Prepare the Day 0 Configuration File

You can prepare a Day 0 configuration file before you launch the Firewall Management Center Virtual. The Day 0 configuration is a text file that contains the initial configuration data that gets applied at the time a virtual machine is deployed. This initial configuration is placed into a text file named “day0-config” in a working directory you chose, and is manipulated into a day0.iso file that is mounted and read on first boot.

Note The day0.iso file must be available during first boot.

If you deploy with a Day 0 configuration file, the process allows you to perform the entire initial setup for the Firewall Management Center Virtual appliance. You can specify:

- EULA acceptance
- A host name for the system
- A new administrator password for the admin account
- Network settings that allow the appliance to communicate on your management network If you deploy without a Day 0 configuration file, you must configure System-required settings after launch; see Deploy Without Using the Day 0 Configuration File, on page 31 for more information.

Note We use Linux in this example, but there are similar utilities for Windows.

- Leave both DNS entries empty to use the default Cisco Umbrella DNS servers. To operate in a non-DNS environment, set both entries to “None” (not case sensitive).

Procedure

Step 1 Enter the CLI configuration for the Firewall Management Center Virtual network settings in a text file called “day0-config”.

Example:

```
#FMC
{
    "EULA": "accept",
    "Hostname": "FMC-Production",
    "AdminPassword": "r2M$9^Uk69##",
    "DNS1": "10.1.1.5",
    "DNS2": "192.168.1.67",

    "IPv4Mode": "manual",
    "IPv4Addr": "10.12.129.45",
    "IPv4Mask": "255.255.0.0",
    "IPv4Gw": "10.12.0.1",
    "IPv6Mode": "enabled",
    "IPv6Addr": "2001:db8::a111:b221:1:abca/96",
    "IPv6Mask": "",
```

```
    "IPv6Gw": "",
}
```

Step 2 Generate the virtual CD-ROM by converting the text file to an ISO file:

Example:

```
/usr/bin/genisoimage -r -o day0.iso day0-config
```

or

Example:

```
/usr/bin/mkisofs -r -o day0.iso day0-config
```

Step 3 Repeat to create unique default configuration files for each Firewall Management Center Virtual you want to deploy.

What to do next

- If using virt-install, add the following line to the virt-install command:

  ```
  --disk path=/home/user/day0.iso,format=iso,device=cdrom \
  ```

- If using virt-manager, you can create a virtual CD-ROM using the virt-manager GUI; see Deploy the Firewall Management Center Virtual, on page 30.

Deploy the Firewall Management Center Virtual

You can launch the Firewall Management Center Virtual on KVM using the following methods:

- Using a Deployment Script—Use a virt-install based deployment script to launch the Firewall Management Center Virtual; see Launch Using a Deployment Script, on page 28.
- Using Virtual Machine Manager—Use virt-manager, a graphical tool for creating and managing KVM guest virtual machines, to launch the Firewall Management Center Virtual; see Deploy the Firewall Management Center Virtual, on page 30.

You can also choose to deploy the Firewall Management Center Virtual without the Day 0 configuration file. This requires you to complete the initial setup using the appliance's CLI or the web interface.

Launch Using a Deployment Script

You can use a virt-install based deployment script to launch the Firewall Management Center Virtual.

Before you begin

Be aware that you can optimize performance by selecting the best guest caching mode for your environment. The cache mode in use will affect whether data loss occurs, and the cache mode can also affect disk performance.

Each KVM guest disk interface can have one of the following cache modes specified: *writethrough*, *writeback*, *none*, *directsync*, or *unsafe*. The *writethrough* mode provides read caching; *writeback* provides read and write caching; *directsync* bypasses the host page cache; *unsafe* may cache all content and ignore flush requests from the guest.

- A *cache=writethrough* will help reduce file corruption on KVM guest machines when the host experiences abrupt losses of power. We recommend that you use writethrough mode.
- However, *cache=writethrough* can also affect disk performance due to more disk I/O writes than *cache=none*.
- If you remove the cache parameter on the *--disk* option, the default is *writethrough*.
- Not specifying a cache option may also significantly reduce the time required for the VM creation. This is due to the fact that some older RAID controllers have poor disk caching capability. Hence, disabling disk caching (*cache=none*) and thus defaulting to *writethrough*, helps ensure data integrity.

Procedure

Step 1 Create a virt-install script called “virt_install_fmc.sh”.

The name of the Firewall Management Center Virtual instance must be unique across all other virtual machines (VMs) on this KVM host. The Firewall Management Center Virtual can support one network interface. The virtual NIC must be Virtio.

Example:

```
virt-install \
    --connect=qemu:///system \
    --network network=default,model=virtio \
    --name=fmcv \
    --arch=x86_64 \
    --cpu host \
    --vcpus=4 \
    --ram=28672 \
    --os-type=generic \
    --virt-type=kvm \
    --import \
    --watchdog i6300esb,action=reset \
    --disk path=<fmc_filename>.qcow2,format=qcow2,device=disk,bus=virtio,cache=writethrough \
    --disk path=<day0_filename>.iso,format=iso,device=cdrom \
    --console pty,target_type=serial \
    --serial tcp,host=127.0.0.1:<port>,mode=bind,protocol=telnet \
    --force
```

Note In the deployment script, ensure to set the value of the --os-type parameter to **generic** for the deployment process to correctly identify the platform on which the virtual instance is deployed.

Step 2 Run the virt_install script:

Example:

```
/usr/bin/virt_install_fmc.sh
Starting install...
Creating domain...
```

A window appears displaying the console of the VM. You can see that the VM is booting. It takes a few minutes for the VM to boot. Once the VM stops booting you can issue CLI commands from the console screen.

Deploy the Firewall Management Center Virtual

Use virt-manager, also known as Virtual Machine Manager, to launch the Firewall Management Center Virtual. virt-manager is a graphical tool for creating and managing guest virtual machines.

Procedure

Step 1 Start virt-manager (**Applications** > **System Tools** > **Virtual Machine Manager**).

You may be asked to select the hypervisor and/or enter your root password.

Step 2 Click the button in the top left corner to open the **New VM** wizard.

Step 3 Enter the virtual machine details:

a) For the operating system, select **Import existing disk image**.

This method allows you to import a disk image (containing a pre-installed, bootable operating system) to it.

b) Click **Forward** to continue.

Step 4 Load the disk image:

a) Click **Browse...** to select the image file.
b) Choose *Use Generic* for the **OS type**.
c) Click **Forward** to continue.

Step 5 Configure the memory and CPU options:

a) Set **Memory (RAM)** to *28672*.
b) Set **CPUs** to *4*.
c) Click **Forward** to continue.

Step 6 Check the **Customize configuration before install** box, specify a **Name**, then click **Finish**.

Doing so opens another wizard that allows you to add, remove, and configure the virtual machine's hardware settings.

Step 7 Modify the CPU configuration.

From the left panel, select Processor, then select **Configuration** > **Copy host CPU configuration**.

This applies the physical host's CPU model and configuration to your virtual machine.

Step 8 8. Configure the Virtual Disk:

a) From the left panel, select **Disk 1**.
b) Select **Advanced options**.

c) Set the **Disk bus** to *Virtio*.
d) Set the **Storage format** to *qcow2*.

Step 9 Configure a serial console:

a) From the left panel, select **Console**.
b) Select **Remove** to remove the default console.
c) Click **Add Hardware** to add a serial device.
d) For **Device Type**, select *TCP net console (tcp)*.
e) For **Mode**, select *Server mode (bind)*.
f) For **Host**, enter **0.0.0.0** for the IP address and enter a unique **Port** number.
g) Check the **Use Telnet** box.
h) Configure device parameters.

Step 10 Configure a watchdog device to automatically trigger some action when the KVM guest hangs or crashes:

a) Click **Add Hardware** to add a watchdog device.
b) For **Model**, select *default*.
c) For **Action**, select *Forcefully reset the guest*.

Step 11 Configure the virtual network interface.

Choose **macvtap** or specify a shared device name (use a bridge name).

Note By default, the Firewall Management Center Virtual instance launches with one interface, which you can then configure.

Step 12 If deploying using a Day 0 configuration file, create a virtual CD-ROM for the ISO:

a) Click **Add Hardware**.
b) Select **Storage**.
c) Click **Select managed or other existing storage** and browse to the location of the ISO file.
d) For **Device type**, select *IDE CDROM*.

Step 13 After configuring the virtual machine's hardware, click **Apply**.

Step 14 Click **Begin installation** for virt-manager to create the virtual machine with your specified hardware settings.

Deploy Without Using the Day 0 Configuration File

For all Firewall Management Centers, you must complete a setup process that allows the appliance to communicate on your management network. If you deploy without a Day 0 configuration file, setting up the Firewall Management Center Virtual is a two-step process:

- After you initialize the Firewall Management Center Virtual, run a script at the appliance console that helps you configure the appliance to communicate on your management network.
- Then, complete the setup process using a computer on your management network to browse to the web interface of the Firewall Management Center Virtual.

Configure Network Settings Using a Script

The following procedure describes how you complete the initial setup on the Firewall Management Center Virtual using the CLI.

Procedure

Step 1 At the console, log into the Firewall Management Center Virtual appliance. Use **admin** as the username and **Admin123** as the password.

Step 2 At the admin prompt, run the following script:

Example:

```
sudo /usr/local/sf/bin/configure-network
```

On first connection to the Firewall Management Center Virtual you are prompted for post-boot configuration.

Step 3 Follow the script's prompts.

Configure (or disable) IPv4 management settings first, then IPv6. If you manually specify network settings, you must enter IPv4 or IPv6 address.

Step 4 Confirm that your settings are correct.

Step 5 Log out of the appliance.

What to do next

- Complete the setup process using a computer on your management network to browse to the web interface of the Firewall Management Center Virtual.

Perform Initial Setup Using the Web Interface

The following procedure describes how you complete the initial setup on the Firewall Management Center Virtual using the web interface.

Procedure

Step 1 Direct your browser to default IP address of the Firewall Management Center Virtual's management interface:

Example:

```
https://192.168.45.45
```

Step 2 Log into the Firewall Management Center Virtual appliance. Use **admin** as the username and **Admin123** as the password. The setup page appears.

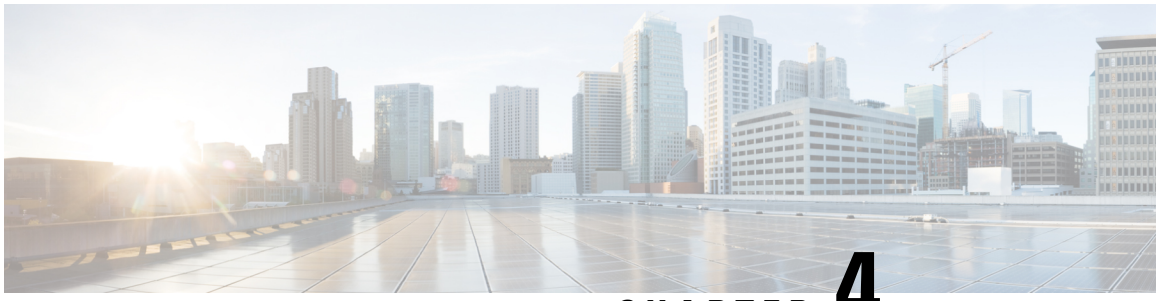
The setup page appears. You must change the administrator password, specify network settings if you haven't already, and accept the EULA.

Step 3 When you are finished, click **Apply**. The Firewall Management Center Virtual is configured according to your selections. After an intermediate page appears, you are logged into the web interface as the admin user, which has the Administrator role.

The Firewall Management Center Virtual is configured according to your selections. After an intermediate page appears, you are logged into the web interface as the admin user, which has the Administrator role.

What to do next

- For more information about the initial setup of the Firewall Management Center Virtual, seeFirewall Management Center Virtual Initial Setup, on page 137
- For an overview of the next steps needed in your Firewall Management Center Virtual deployment, see the chapter Firewall Management Center Virtual Initial Administration and Configuration, on page 147.



CHAPTER 4

Deploy the Firewall Management Center Virtual on AWS

Amazon Virtual Private Cloud (Amazon VPC) enables you to launch Amazon Web Services (AWS) resources into a virtual network that you define. This virtual network closely resembles a traditional network that might operate in your own data center, with the benefits of using the scalable infrastructure of AWS.

You can deploy the Firewall Management Center Virtual on the AWS Cloud.

- Overview, on page 35
- Guidelines and Limitations, on page 38
- Configure the AWS Environment, on page 39
- Deploy the Firewall Management Center Virtual, on page 44

Overview

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 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. See Table 7: AWS Supported Instance Types for the Firewall Management Center Virtual, on page 36.

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

The following table summarizes the AWS instance types that the Firewall Management Center Virtual supports; those that Versions 6.5.x and earlier support, and those that Version 6.6.0+ support.

Note Version 6.6 adds support for the C5 instance types shown in the following table. Larger instance types provide more CPU resources to your AWS VMs for increased performance, and some allow for more network interfaces.

Table 7: AWS Supported Instance Types for the Firewall Management Center Virtual

Platform	Version 7.0+	vCPUs	Memory (GB)	Maximum Number of Interfaces	Version 6.6.0+	vCPUs	Memory (GB)	Maximum Number of Interfaces	Version 6.5.x and earlier	vCPUs	Memory (GB)	Maximum Number of Interfaces
Firewall Management Center Virtual	c5.4xlarge	16	42	8	c3.4xlarge	16	30	8	c3.xlarge*	4	7.5	4
	c4.4xlarge	16	32	8	c4.4xlarge	16	30	8	c3.2xlarge*	8	15	4
	c5.4xlarge	16	32	8	c5.4xlarge	16	32	8	c3.4xlarge	16	30	8
	c6i.4xlarge	16	32	8	c6i.4xlarge	16	32	8	c4.xlarge*	4	7.5	4
	m6a.2xlarge	8	32	4	c6a.4xlarge	16	32	8	c4.2xlarge*	8	15	4
	m6in.4xlarge	16	64	8	c6in.4xlarge	16	32	8	c4.4xlarge	16	30	8
	c6i.2xlarge	8	64	4	-	-	-	-	-	-	-	-
	c6in.8xlarge	8	64	8	-	-	-	-	-	-	-	-
	c7i.4xlarge	16	32	8	-	-	-	-	-	-	-	-
	c7a.4xlarge	16	32	8	-	-	-	-	-	-	-	-
	c7i.4xlarge	16	32	8	-	-	-	-	-	-	-	-
	m7i.2xlarge	8	32	4	-	-	-	-	-	-	-	-
	m7i.4xlarge	16	64	8	-	-	-	-	-	-	-	-
	m7a.2xlarge	8	32	4	-	-	-	-	-	-	-	-
	m7a.4xlarge	16	64	8	-	-	-	-	-	-	-	-
	*Note that the Firewall Management Center Virtual will not support these instance types on Version 6.6.0 and above. Beginning with Version 6.6.0, you must deploy the Firewall Management Center Virtual (any version) using an instance with at least 28 GB RAM. See Deprecated Instanc Types and Resizing Instance Types, on page 37 for more information.											

Table 8: AWS Supported Instance Types for the Firewall Management Center Virtual 300

Platform	Version 7.1.0+
Firewall Management Center Virtual 300 (FMCv300)	c5.9xlarge: 36 vCPUs, 72 GB SSD storage: 2000 GB

Deprecated Instance Types

You can continue running your current Version 6.5.x and earlier Firewall Management Center Virtual deployments, but you will not be able to launch the new Firewall Management Center Virtual deployments (any version) using these instance types:

- c3.xlarge—4 vCPUs, 7.5 GB (DISABLED for the Firewall Management Center Virtual after Version 6.6.0+)
- c3.2xlarge—8 vCPUs, 15 GB (DISABLED for the Firewall Management Center Virtual after Version 6.6.0+)
- c4.xlarge—4 vCPUs, 7.5 GB (DISABLED for the Firewall Management Center Virtual after Version 6.6.0+)
- c4.2xlarge—8 vCPUs, 15 GB (DISABLED for the Firewall Management Center Virtual after Version 6.6.0+)

Resizing Instance Types

Because the upgrade path from any earlier version of Firewall Management Center Virtual (6.2.x, 6.3.x, 6.4.x, and 6.5.x) to Version 6.6.0 includes the 28 GB RAM memory check, you need to resize your current instance type to one that supports Version 6.6.0 (see Table 7: AWS Supported Instance Types for the Firewall Management Center Virtual, on page 36).

You can resize an instance if the current instance type and the new instance type that you want are compatible. For the Firewall Management Center Virtual deployments:

- Resize any c3.xlarge or c3.2xlarge to the c3.4xlarge instance type.
- Resize any c4.xlarge or c4.2xlarge to the c4.4xlarge instance type.

Be aware of the following before resizing your instance:

- You must stop your instance before you change instance types.
- Verify that your current instance type is compatible with the new instance type that you choose.
- If this instance has an instance store volume, any data on it is lost when the instance is stopped. Migrate your instance store-backed instance before you resize.
- If you're not using an Elastic IP address, the public IP address is released when you stop the instance.

For instructions on how to resize your instance, see the AWS documentation “Changing the Instance Type” (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-resize.html).

AWS Solution Overview

AWS is a collection of remote computing services offered by Amazon.com, also called web services, that make up a cloud-computing platform. These services operate from 11 geographical regions across the world. In general, you should become familiar with the following AWS services when deploying the Firewall Management Center Virtual:

- Amazon Elastic Compute Cloud (EC2)—a web service that enables you to rent virtual computers to launch and manage your own applications and service, such as a firewall, in Amazon's data centers.

- Amazon Virtual Private Cloud (VPC)—a web service that enables you to configure an isolated private network that exists within the Amazon public cloud. You run you EC2 instances within a VPC.
- Amazon Simple Storage Service (S3)—a web service that provides you with a data storage infrastructure.

You create an account on AWS, set up the VPC and EC2 components (using either the AWS Wizards or manual configuration), and chose an Amazon Machine Image (AMI) instance. The AMI is a template that contains the software configuration needed to launch your instance.

Note The AMI images are not available for download outside of the AWS environment.

Guidelines and Limitations

Supported Features (7.1.0+)

- **Management Center Virtual 300 (FMCv300) for AWS**—A new scaled Firewall Management Center Virtual image is available on the AWS platform that supports managing up to 300 devices and has higher disk capacity.
- Firewall Management Center Virtual high availability (HA) is supported.

Prerequisites

The following prerequisites pertain to the Firewall Management Center Virtual on AWS:

- An Amazon account. You can create one at aws.amazon.com.
- A Cisco Smart Account. You can create one at Cisco Software Central (https://software.cisco.com/).
- License the Firewall Management Center Virtual. See Firewall Management Center Virtual Licenses, on page 4 for general guidelines about virtual platform licenses; see “Licensing the System” in the *Secure Firewall Management Center Configuration Guide* for more detailed information about how to manage licenses.
- The Firewall Management Center Virtual interface requirements:
  - Management interface.
- Communication Paths:
  - Public/elastic IPs for access into the Firewall Management Center Virtual.
- For the Firewall Management Center Virtual and System compatibility, see the Cisco Secure Firewall Threat Defense Compatibility Guide.

Guidelines

The following guidelines pertain to the Firewall Management Center Virtual on AWS:

- Deployment in the Virtual Private Cloud (VPC).

- Enhanced networking (SR-IOV) where available.
- Deployment from Amazon Marketplace.
- Maximum of four vCPUs per instance.
- User deployment of L3 networks.
- IPv6 is supported.

Limitations

The following limitations pertain to the Firewall Management Center Virtual on AWS:

- The 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.
- Any IP address configuration (either from CLI or Firewall Management Center) must match what is created in the AWS console; you should note your configurations during deployment.
- You cannot add interfaces after boot.
- Cloning/snapshots are currently not supported.
- Transport Layer Security (TLS) Server Identity Discovery is not supported with Geneve single-arm setup on AWS.

Configure the AWS Environment

To deploy the Firewall Management Center Virtual on AWS you need to configure an Amazon VPC with your deployment-specific requirements and settings. In most situations a setup wizard can guide you through your setup. AWS provides online documentation where you can find useful information about the services ranging from introductions to advanced features. See Getting Started with AWS for more information.

For greater control over your AWS setup, the following sections offer a guide to your VPC and EC2 configurations prior to launching instances of the Firewall Management Center Virtual:

- Create the VPC, on page 39
- Add the Internet Gateway, on page 40
- Add Subnets, on page 41
- Add a Route Table, on page 41
- Create a Security Group, on page 42
- Create Network Interfaces, on page 43
- Create Elastic IPs, on page 44

Create the VPC

A virtual private cloud (VPC) is a virtual network dedicated to your AWS account. It is logically isolated from other virtual networks in the AWS cloud. You can launch your AWS resources, such as Firewall

Management Center Virtual instances, into your VPC. You can configure your VPC; you can select its IP address range, create subnets, and configure route tables, network gateways, and security settings.

Before you begin

- Create your AWS account.
- Confirm that AMIs are available for the Firewall Management Center Virtual instances.

Procedure

Step 1 Log into aws.amazon.com and choose your region.

AWS is divided into multiple regions that are isolated from each other. The region is displayed in the upper right corner of your screen. Resources in one region do not appear in another region. Check periodically to make sure you are in the intended region.

Step 2 Click **Services** > **VPC**.

Step 3 Click **VPC Dashboard** > **Your VPCs**.

Step 4 Click **Create VPC**.

Step 5 Enter the following in the **Create VPC** dialog box:

a) A user-defined **Name tag** to identify the VPC.

b) A **CIDR block** of IP addresses. CIDR (Classless Inter-Domain Routing) notation is a compact representation of an IP address and its associated routing prefix. For example, 10.0.0.0/24.

c) A **Tenancy** setting of Default to ensure that instances launched in this VPC use the tenancy attribute specified at launch.

Step 6 Click **Yes, Create** to create your VPC.

What to do next

Add an Internet gateway to your VPC as described in the next section.

Add the Internet Gateway

You can add an Internet gateway to connect your VPC to the Internet. You can route traffic for IP addresses outside your VPC to the Internet gateway.

Before you begin

- Create a VPC for your Firewall Management Center Virtual instances.

Procedure

Step 1 Click **Services** > **VPC**.

Step 2 Click **VPC Dashboard** > **Internet Gateways**, and then click **Create Internet Gateway**.

Step 3 Enter a user-defined Name tag to identify the gateway and click Yes, Create to create the gateway.

Step 4 Select the gateway created in the previous step.

Step 5 Click **Attach to VPC** and select the VPC you created previously.

Step 6 Click **Yes, Attach** to attach the gateway to your VPC.

By default, the instances launched on the VPC cannot communicate with the Internet until a gateway is created and attached to the VPC.

What to do next

Add subnets to your VPC as described in the next section.

Add Subnets

You can segment the IP address range of your VPC that the Firewall Management Center Virtual instances can be attached to. You can create subnets to group instances according to security and operational needs. For the Firewall Threat Defense Virtual you need to create a subnet for management as well as subnets for traffic.

Procedure

Step 1 Click **Services** > **VPC**.

Step 2 Click **VPC Dashboard** > **Subnets**, and then click **Create Subnet**.

Step 3 Enter the following in the **Create Subnet** dialog box:

a) A user-defined **Name tag** to identify the subnet.

b) A **VPC** to use for this subnet.

c) The **Availability Zone** where this subnet will reside. Select No Preference to let Amazon select the zone.

d) A **CIDR block** of IP addresses. The range of IP addresses in the subnet must be a subset of the range of IP addresses in the VPC. Block sizes must be between a /16 network mask and a /28 network mask. The size of the subnet can equal the size of the VPC.

Step 4 Click **Yes, Create** to create your subnet.

Step 5 Repeat for as many subnets required. Create a separate subnet for management traffic and create as many subnets as needed for data traffic.

What to do next

Add a route table to your VPC as described in the next section.

Add a Route Table

You can attach a route table to the gateway you configured for your VPC. You can also associate multiple subnets with a single route table, but a subnet can be associated with only one route table at a time.

Procedure

Step 1 Click **Services** > **VPC**.

Step 2 Click **VPC Dashboard** > **Route Tables**, and then click **Create Route Table**.

Step 3 Enter a user-defined **Name tag** to identify the route table.

Step 4 Select the **VPC** from the drop-down list that will use this route table.

Step 5 Click **Yes, Create** to create your route table.

Step 6 Select the route table that you just created.

Step 7 Click the **Routes** tab to display the route information in the details pane.

Step 8 Click **Edit**, then click **Add another route**.

a) In the **Destination** column, enter **0.0.0.0/0**.

b) In the **Target** column, select the Internet Gateway you created above.

Step 9 Click **Save**.

Step 10 Click the **Subnet Associations** tab and click **Edit**.

Step 11 Check the box next to the subnet to be used for the Firewall Management Center Virtual's management interface and click **Save**.

What to do next

Create a security group as described in the next section.

Create a Security Group

You can create a security group with rules specifying allowed protocols, ports and source IP ranges. Multiple security groups can be created with different rules which you can assign to each instance. AWS has detailed documentation on Security Groups if you are not familiar with this feature.

Procedure

Step 1 Click **Services** > **EC2**.

Step 2 Click **EC2 Dashboard** > **Security Groups**.

Step 3 Click **Create Security Group**.

Step 4 Enter the following in the **Create Security Group** dialog box:

a) A user-defined **Security group name** to identify the security group.

b) A **Description** for this security group.

c) The **VPC** associated with this security group.

Step 5 Configure **Security group rules**:

a) Click **Create Security Group**.

b) Under the **Inbound** section, click **Add Rule**.

Choose any of the following inbound ports to be opened for access by the internet from the **Type** drop-down list. By default, the **All Traffic** type is selected.

- SSH (22)
- Custom TCP (8305)
- HTTP (443)



Note HTTPS and SSH access is required to manage the Firewall Management Center Virtual from outside AWS. You should specify the Source IP addresses accordingly. Also, if you are configuring both the Firewall Management Center Virtual and Firewall Threat Defense Virtual within the AWS VPC, you should allow the private IP management subnet access.

c) Under the **Outbound** section, click **Add Rule** to add a rule for outbound traffic, or leave the defaults of **All traffic** (for **Type**) and **Anywhere** (for **Destination**).

Step 6 Click **Create security group** to create your security group.

What to do next

Create network interfaces as described in the next section.

Create Network Interfaces

You can create network interfaces for the Firewall Management Center Virtual using static IP addresses. Create network interfaces (external and internal) as needed for your particular deployment.

Procedure

Step 1 Click **Services** > **EC2**.

Step 2 Click **EC2 Dashboard** > **Network Interfaces**.

Step 3 Click **Create Network Interface**.

Step 4 Enter the following in the **Create Network Interface** dialog box:

a) A optional user-defined **Description** for the network interface.

b) Select a **Subnet** from the drop-down list. Make sure to select the subnet of the VPC where you want to create the instance.

c) Enter a **Private IP** address. It is recommended to use a static IP address rather than **auto-assign**.

d) Select one or more **Security groups**. Make sure the security group has all the required ports open.

Step 5 Click **Yes, Create** to create your network interface.

Step 6 Select the network interface that you just created.

Step 7 Right-click and select **Change Source/Dest. Check**.

Step 8 Choose **Disabled**, then click **Save**.

Repeat this for any network interfaces you create.

What to do next

Create elastic IP addresses as described in the next section.

Create Elastic IPs

When an instance is created, a public IP address is associated with the instance. That public IP address changes automatically when you STOP and START the instance. To resolve this issue, assign a persistent public IP address to the instance using Elastic IP addressing. Elastic IPs are reserved public IPs that are used for remote access to the Firewall Management Center Virtual as well as other instances. AWS has detailed documentation on Elastic IPs if you are not familiar with this feature.



Note At a minimum, you want to create one elastic IP addresses for the Firewall Management Center Virtual and two elastic IP addresses for the Firewall Threat Defense Virtual management and diagnostic interfaces.

Procedure

Step 1 Click **Services** > **EC2**.

Step 2 Click **EC2 Dashboard** > **Elastic IPs**.

Step 3 Click **Allocate New Address**.

Repeat this step for as many elastic/public IPs that you require.

Step 4 Click **Yes, Allocate** to create your elastic IP.

Step 5 Repeat for as many elastic IPs required for your deployment.

What to do next

Deploy the Firewall Management Center Virtual as described in the next section.

Deploy the Firewall Management Center Virtual

Before you begin

- Configure AWS VPC and EC2 elements as described in Configuring Your AWS Environment.
- Confirm that an AMI is available for the Firewall Management Center Virtual instances.

Note The default admin password is the AWS Instance ID, unless you define a default password with user data (**Advanced Details** > **User Data**) during the initial deployment.

Procedure

Step 1 Go to https://aws.amazon.com/marketplace (Amazon Marketplace) and sign in.

Step 2 After you are logged in to the Amazon Marketplace, click the link provided for the Firewall Management Center Virtual.

Note If you were previously in AWS, you may need to sign out and then sign back in for the link to work.

Step 3 Click **Continue**, then click the **Manual Launch** tab.

Step 4 Click **Accept Terms**.

Step 5 Click **Launch with EC2 Console** in your desired region

Step 6 Choose an **Instance Type** supported by the Firewall Management Center Virtual; see About Deployment On the AWS Cloud for the supported instance types.

Step 7 Click the **Next: Configure Instance Details** button at the bottom of the screen:

a) Change the **Network** to match your previously created VPC.

b) Change the **Subnet** to match your previously created management subnet. You can specify an IP address or use auto-generate.

c) Under **Advanced Details** > **User Data**, add the default login information.

Modify the example below to match your requirements for device name and password.

Sample login configuration:

```
#FMC
{
"AdminPassword": "<enter_your_password>",
"Hostname": "<Hostname-vFMC>"
}
```

Caution Use only plain text when entering data in the **Advanced Details** field. If you copy this information from a text editor, make sure you copy only as plain text. If you copy any Unicode data into the **Advanced Details** field, including white space, the instance may be corrupted and you will have to terminate the instance and re-create it.

In Version 7.0 and greater, the default admin password is the AWS Instance ID, unless you define a default password with user data (**Advanced Details** > **User Data**) during the initial deployment.

In earlier releases the default admin password was **Admin123**.

Step 8 Click **Next: Add Storage** to configure your storage device settings.

Edit the settings of the root volume so the volume Size (GiB) is 250 GiB. Less than 250 GiB will limit event storage and is not supported.

Step 9 Click **Next: Tag Instance**.

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with **Key** = Name and **Value** = Management.

Step 10 Select **Next: Configure Security Group**.

Step 11 Click **Select an existing Security Group** and choose the previously configured Security Group, or create a new Security Group; see AWS documentation for more information on creating Security Groups.

Step 12 Click **Review and Launch**.

Step 13 Click **Launch**.

Step 14 Select an existing key pair or create a new key pair.

Note You can select an existing key pair, or create a new key pair. The key pair consists of a public key that AWS stores and a private key file that the user stores. Together they allow you to connect to your instance securely. Be sure to save the key pair to a known location, as it will may be required to connect to the instance.

Step 15 Click **Launch Instances**.

Step 16 Click **EC2 Dashboard** > **Elastic IPs** and find a previously allocated IP, or allocate a new one.

Step 17 Select the elastic IP, right-click and select **Associate Address**.

Locate the Instance or Network Interface to select, then click Associate.

Step 18 Click **EC2 Dashboard** > **Instances**.

Step 19 The Firewall Management Center Virtual Instance state will show "running" and Status checks will show pass for "2/2 checks" after only a few minutes. However, deployment and initial setup processes will take approximately 30 to 40 minutes to complete. To view the status, right-click the Instance, then select Instance **Settings** > **Get Instance Screenshot**.

When setup is complete (after approximately 30 to 40 minutes), the **Instance Screenshot** should show a message similar to "Cisco Secure Firewall Management Center for AWS vW.X.Y (build ZZ)" and possibly followed by some additional lines of output.

You should then be able to log in to the newly created the Firewall Management Center Virtual using SSH or HTTPs. Actual deployment times may vary depending on the AWS load in your region.

You can access the Firewall Management Center Virtual using SSH:

```
ssh -i <key_pair>.pem admin@<Public_Elastic_IP>
```

SSH authentication is handled by a key pair. No password is required. If you are prompted for a password then setup is still running.

You can also access the Firewall Management Center Virtual using HTTPS:

```
https//<Public_Elastic_IP>
```

Note If you see a "system startup processes are still running" then setup is not yet complete.

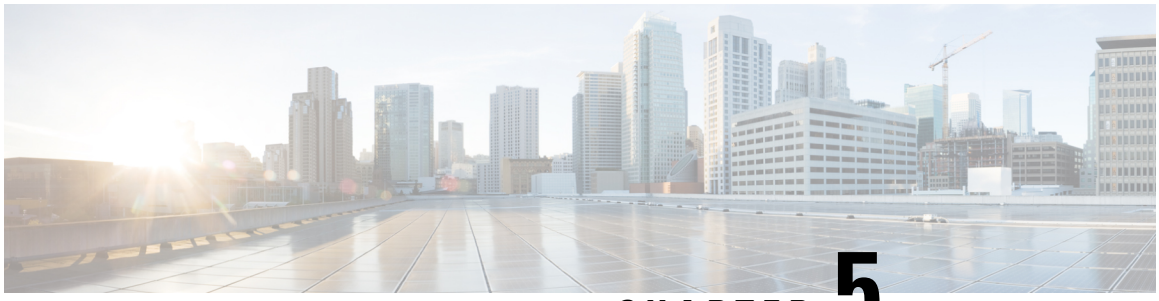
If you get no response from SSH or HTTPS, double check these items:

- Make sure deployment is complete. The Firewall Management Center Virtual VM Instance Screenshot should show a message similar to “Cisco Secure Firewall Management Center for AWS vW.X.Y (build ZZ)” and possibly followed by some additional lines of output.
- Make sure you have an Elastic IP and that it is associated with the Firewall Management Center's management network interface (eni) and that you are connecting to that IP address.
- Make sure there is an Internet Gateway (igw) associated with your VPC.
- Make sure your management subnet has a route table associated with it.
- Make sure the route table associated with your Management subnet has a route for “0.0.0.0/0” that points to your Internet gateway (igw).
- Make sure your Security Group allows incoming SSH and/or HTTPS from the IP addresses you are connecting from.

What to do next

Configuring Policies and Device Settings

After you install the Firewall Threat Defense Virtual and add the device to the Management Center, you can use the Firewall Management Center user interface to configure device management settings for the Firewall Threat Defense Virtual running on AWS and to configure and apply access control policies and other related policies to manage traffic using your Firewall Threat Defense Virtual device. The security policy controls the services provided by the Firewall Threat Defense Virtual, such as Next Generation IPS filtering and application filtering. You configure the security policy on the Firewall Threat Defense Virtual using the Firewall Management Center. For information about how to configure the security policy, see the Configuration Guide or the online help in Management Center.



CHAPTER 5

Deploy the Firewall Management Center Virtual on Azure

You can deploy the Firewall Management Center Virtual as a virtual machine on the Microsoft Azure public cloud.

Important The Firewall Management Center Virtual is supported on Microsoft Azure starting with Cisco software version 6.4 and later.

- Overview, on page 49
- Prerequisites, on page 51
- Guidelines and Limitations, on page 51
- Resources Created During Deployment, on page 53
- Deploy the Firewall Management Center Virtual, on page 54
- Deploy the Azure Marketplace offers in the restricted Azure Private Marketplace environment, on page 61
- Deploy the IPv6 Supported on Azure, on page 63
- Verify the Firewall Management Center Virtual Deployment, on page 74
- Monitoring and Troubleshooting, on page 76
- Feature History, on page 77

Overview

You deploy the Firewall Management Center Virtual in Microsoft Azure using a solution template available in the Azure Marketplace. When you deploy the Firewall Management Center Virtual using the Azure portal you can use an existing empty resource group and storage account (or create them new). The solution template walks you through a set of configuration parameters that provide the initial setup of your Firewall Management Center Virtual, allowing you to login to the Firewall Management Center Virtual web interface after first boot.

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 As of the Version 6.6.0 release, lower-memory VM sizes for cloud-based Firewall Management Center Virtual deployments (AWS, Azure) are fully deprecated. You cannot create new Firewall Management Center Virtual instances using them, even for earlier versions. You can continue running existing VM sizes. See Table 10: Azure Supported VM Size for the FMCv300, on page 51.

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

The Firewall Management Center Virtual on Azure must be deployed in a virtual network (VNet) using the Resource Manager deployment mode. You can deploy the Firewall Management Center Virtual in the standard Azure public cloud environment. The Firewall Management Center Virtual in the Azure Marketplace supports the Bring Your Own License (BYOL) model.

The following table summarizes the Azure VM sizes that the Firewall Management Center Virtual supports; those that Versions 6.5.x and earlier support, and those that Version 6.6.0+ support.

Table 9: Azure Supported VM Sizes and Firewall Management Center Virtual Versions

Azure VM Size	Attributes		Firewall Management Center Virtual Version
	vCPUs	Memory (GB)	
Standard_D3_v2	4	14	6.5 or earlier
Standard_D4_v2	8	28	6.6 or later
Standard_D8_v4	8	32	7.7.10 or later
Standard_D16_v4	16	64	7.7.10 or later
Standard_D8s_v4	8	32	7.7.10 or later
Standard_D16s_v4	16	64	7.7.10 or later
Standard_D8_v5	8	32	7.7.10 or later
Standard_D16_v5	16	64	7.7.10 or later
Standard_D8s_v5	8	32	7.7.10 or later
Standard_D16s_v5	16	64	7.7.10 or later
Standard_F16s_v2	16	32	10.1.0 or later

Table 10: Azure Supported VM Size for the FMCv300

Platform	Version 7.3.0
Management Center Virtual 300 (FMCv300)	Standard_D32ds_v5: 32 vCPUs, 128 GB

Deprecated VM Sizes

You can continue running your current Version 6.5.x and earlier the Firewall Management Center Virtual deployments using Standard_D3_v2, but you will not be able to launch new Firewall Management Center Virtual deployments (any version) using this VM size.

Resizing VM

Because the upgrade path from any earlier version of Firewall Management Center Virtual (6.2.x, 6.3.x, 6.4.x, and 6.5.x) to Version 6.6.0 includes the 28 GB RAM memory check, if you are using the Standard_D3_v2, you need to resize your VM to Standard_D4_v2 (see Table 10: Azure Supported VM Size for the FMCv300, on page 51).

You can use the Azure portal or PowerShell to resize your VM. If the virtual machine is currently running, changing its size will cause it to be restarted. Stopping the virtual machine may reveal additional sizes.

For instructions on how to resize your VM, see the Azure documentation “Resize a Windows VM” (https://docs.microsoft.com/en-us/azure/virtual-machines/windows/resize-vm).

Prerequisites

Support for the Firewall Management Center Virtual on Microsoft Azure is new with the release of version 6.4.0. For the Firewall Management Center Virtual and System compatibility, see Cisco Secure Firewall Threat Defense Compatibility Guide.

Verify the following before you deploy the Firewall Management Center Virtual in Azure:

- Create an account on Azure.com.

  After you create an account on Microsoft Azure, you can log in, search the marketplace for Firewall Management Center Virtual, and choose the “Firewall Management Center BYOL” offering.

- A Cisco Smart Account. You can create one at Cisco Software Central (https://software.cisco.com/).

Guidelines and Limitations

Supported Features

- Supported Azure VM sizes:
  - Standard_D3_v2—4 vCPUs, 14GB memory, 250GB disk size
  - Standard_D4_v2—8 vCPUs, 28GB memory, 400GB disk size
  - Standard_D32ds_v5: 32 vCPUs, 128 GB memory, 2 TB disk size - with FMCv300

Licensing

The Firewall Management Center Virtual in the Azure public marketplace supports the Bring Your Own License (BYOL) model. For the Firewall Management Center Virtual, this 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 Virtual. For example, you can purchase licenses that enable you to manage two devices, 10 devices, or 25 devices.

- Licensing modes:
  - Smart License only

For licensing details, see *Licensing the System* in the Secure Firewall Management Center Configuration Guide for more information about how to manage licenses; see Cisco Secure Firewall Management Center Feature Licenses for an overview of feature licenses for the System, including helpful links.

System Shut Down and Restart

Do not use the **Restart** and **Stop** controls on the Azure Virtual machine overview page to power on the Firewall Management Center Virtual VM. These are not graceful shutdown mechanisms and can lead to database corruption.

Use the **System** > **Configuration** options available from the Firewall Management Center Virtual's Web interface to shut down or restart the virtual appliance.

Use the `shutdown` and `restart` commands from the Firewall Management Center Virtual's command line interface to shut down or restart the appliance.

High Availability support

- From Secure Firewall version 7.4.2, High Availability (HA) is supported on the following Managament Center Virtual models on Azure: FMCv10, FMCv25, and FMCv300.
- The two Firewall Management Center Virtual appliances in a high availability configuration must be the same model. You cannot pair the FMCv10 with the FMCv300.
- To establish the Firewall Management Center Virtual HA, Firewall Management Center Virtual requires an extra management center virtual license entitlement for each Secure Firewall Threat Defense device that it manages in the HA configuration. However, the required Firewall Threat Defense feature license entitlement for each 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 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 *High Availability* in the Secure Firewall Management Center Device Configuration Guide for more information and guidelines about high availability.

Unsupported Features

- Licensing modes:
  - Pay As You Go (PAYG) licensing.
  - Permanent License Reservation (PLR).

- Management
  - Azure portal “reset password” function.
  - Console-based password recovery; because the user does not have real-time access to the console, password recovery is not possible. It is not possible to boot the password recovery image. The only recourse is to deploy a new Firewall Management Center Virtual VM.
- VM import/export
- HA is not supported on Secure Firewall version 7.4.1 and earlier versions.
- Gen 2 VM generation on Azure
- Re-sizing the VM after deployment
- Migration or update of the Azure Storage SKU for the OS Disk of the VM from premium to standard SKU and vice versa

Resources Created During Deployment

When you deploy the Firewall Management Center Virtual in Azure the following resources are created:

- The Firewall Management Center Virtual Machine with a single interface (requires a new or an existing virtual network with 1 subnet).
- A Resource Group.

  The Firewall Management Center Virtual is always deployed into a new Resource Group. However, you can attach it to an existing Virtual Network in another Resource Group.
- A security group named *vm name*-mgmt-SecurityGroup.

  The security group will be attached to the VM’s Nic0.

  The security group includes rules to allow SSH (TCP port 22) and the management traffic for the Firewall Management Center interface (TCP port 8305). You can modify these values after deployment.
- A Public IP Address (named according to the value you chose during deployment).

  The public IP address is associated with VM Nic0, which maps to Management.



Note You can create a new public IP or choose an existing one. You can also choose **NONE**. Without a public IP address, any communication to the Firewall Management Center Virtual must originate within the Azure virtual network

- A Routing Table for the subnet (updated if it already exists).
- A boot diagnostics file in the selected storage account.

  The boot diagnostics file will be in Blobs (binary large objects).
- Two files in the selected storage account under Blobs and container VHDs named *VM name*-disk.vhd and *VM name*-<uuid>.status.

- A Storage account (unless you chose an existing storage account).

Important When you delete a VM, you must delete each of these resources individually, except for any resources you want to keep.

Deploy the Firewall Management Center Virtual

You can deploy the Firewall Management Center Virtual in Azure using templates. Cisco provides two kinds of templates:

- **Solution Template in the Azure Marketplace**—Use the solution template available in the Azure Marketplace to deploy the Firewall Management Center Virtual using the Azure portal. You can use an existing resource group and storage account (or create them new) to deploy the virtual appliance. To use the solution template, see Deploy from Azure Marketplace Using the Solution Template, on page 54.
- **ARM Templates in the GitHub Repository**—In addition to the Marketplace-based deployment, Cisco provides Azure Resource Manager (ARM) templates in the GitHub Repository to simplify the process of deploying the Firewall Management Center Virtual on Azure. Using a Managed Image and two JSON files (a Template file and a Parameter file), you can deploy and provision all the resources for the Firewall Management Center Virtual in a single, coordinated operation.

Note While searching for Cisco offers in Marketplace, you may find two different offers with similar names, but different offer types, Application Offer and Virtual Machine Offer.

For marketplace deployments, use ONLY the Application Offers.

Virtual Machine offer (may be visible) with VMSR (Virtual Machine Software Reservations) plan in marketplace. These are specific Multiparty Private Offer plans specifically for channel/resale and should be ignored for regular deployments.

Application Offers available in Marketplace:

- Cisco Secure Firewall Management Center Virtual – BYOL
- Cisco Firepower Management Center 300 Virtual (FMCv300)

Deploy from Azure Marketplace Using the Solution Template

Deploy the Firewall Management Center Virtual from the Azure portal using the solution template available in the Azure Marketplace. The following procedure is a top-level list of steps to set up the Firewall Management Center Virtual in the Microsoft Azure environment. For detailed steps for Azure setup, see Getting Started with Azure.

When you deploy the Firewall Management Center Virtual in Azure it automatically generates various configurations, such as resources, public IP addresses, and route tables. You can further manage these configurations after deployment. For example, you may want to change the Idle Timeout value from the default, which is a low timeout.

Procedure

Step 1 Log in to the Azure portal (https://portal.azure.com) using your Microsoft account credentials.

The Azure portal shows virtual elements associated with the current account and subscription regardless of data center location.

Step 2 Click **Create a Resource**.

Step 3 Search the Marketplace for "Firewall Management Center ", choose the offering, and click **Create**. From Secure Firewall version 7.4.2, FMCv300 is supported on Azure. You will see two separate offerings on the Marketplace - one for Firewall Management Center Virtual, and one for FMCv300.

Step 4 Configure the settings under **Basics**:

a) Enter a name for the virtual machine in the **FMC VM name in Azure** field. This name should be unique within your Azure subscription.

Attention Make sure you do not use an existing name or the deployment will fail.

b) (Optional) Choose the **FMC Software Version** from the dropdown list.

This should default to the latest available version.

c) Enter a username for the Azure account administrator in the **Username for primary account** field.

The name "admin" is reserved in Azure and cannot be used.

Attention The username entered here is for the Azure account, not for the Firewall Management Center Virtual administrator access. Do not use this username to log in to the Firewall Management Center Virtual.

d) Choose an authentication type, either **Password** or **SSH public key**.

If you choose **Password**, enter a password and confirm. The password must be between 12 and 72 characters, and must have 3 of the following: 1 lower case character, 1 upper case character, 1 number, and 1 special character that is not '\' or '-'.

If you choose **SSH public key**, specify the RSA public key of the remote peer.

e) Enter an **FMC Hostname** for the Firewall Management Center Virtual.

f) Enter an **Admin Password**.

This is the password you'll use when you log in to the Firewall Management Center Virtual's Web interface as the administrator to configure the Firewall Management Center Virtual.

g) Choose your **Subscription** type.

Normally there is only one option listed.

h) Create a new **Resource group**.

The Firewall Management Center Virtual should be deployed into a new Resource Group. The option to deploy into an existing Resource Group only works if that existing Resource Group is empty.

However, you can attach the Firewall Management Center Virtual to an existing Virtual Network in another Resource Group when configuring the network options in later steps.

i) Select your geographical **Location**.

You should use the same location for all resources used in this deployment. The Firewall Management Center Virtual, the network, storage accounts, etc. should all use the same location.

j) Click **OK**.

Step 5 Next, complete the initial configuration under **Cisco FMCv Settings**:

a) Confirm the selected **Virtual machine size**, or click the **Change size** link to view the VM size options. Click **Select** to confirm..

Only the supported virtual machine sizes are shown.

b) Configure a **Storage account**. You can use an existing storage account or create a new one.

- Enter a **Name** for the storage account, then click **OK**. The storage account name can only contain lowercase letters and numbers. It cannot contain special characters.
- As of this release the Firewall Management Center Virtual only supports general purpose, standard performance storage.

c) Configure a **Public IP address**. You can use an existing IP or create a new one.

- Click **Create new** to create a new public IP address. Enter a label for the IP address in the **Name** field, select **Standard** for the SKU option, then click **OK**.



Note Azure creates a dynamic public IP address, regardless of the dynamic/static choice made in this step. The public IP may change when the VM is stopped and restarted. If you prefer a fixed IP address, you can edit the public-ip and change it from a dynamic to a static address after the deployment has completed.

- You can choose **NONE** if you don't want to assign a public IP address to the Firewall Management Center Virtual. Without a public IP address, any communication to the Firewall Management Center Virtual must originate within the Azure virtual network.

d) Add a **DNS label** that matches the label of the public IP.

The fully qualified domain name will be your DNS label plus the Azure URL: *<dnslabel>.<location>.cloudapp.azure.com*

e) Choose an existing **Virtual network** or create a new one, the click **OK**.

f) Configure the management subnet for the Firewall Management Center Virtual.

Define a **Management subnet name** and review the **Management subnet prefix**. The recommended subnet name is “management”.

g) Provide **Public inbound ports (mgmt.interface)** input to indicate whether any ports are to be opened for public or not. By default, None is selected.

- Click **None** to create and attach a network security group with Azure's default security rule to the management interface. Selecting this option allows traffic from sources in the same virtual network and from the Azure load balancer.

- Click **Allow selected ports** to view and choose the inbound ports to be opened for acess by the internet. Choose any of the following ports from the **Select Inbound Ports** drop-down list. By default, **HTTPS** is selected.
  - SSH (22)
  - SFTunnel (8305)
  - HTTPs (443)

Note The **Public IP** is not considered for the values of **Allow selected ports** or **Public inbound ports**.

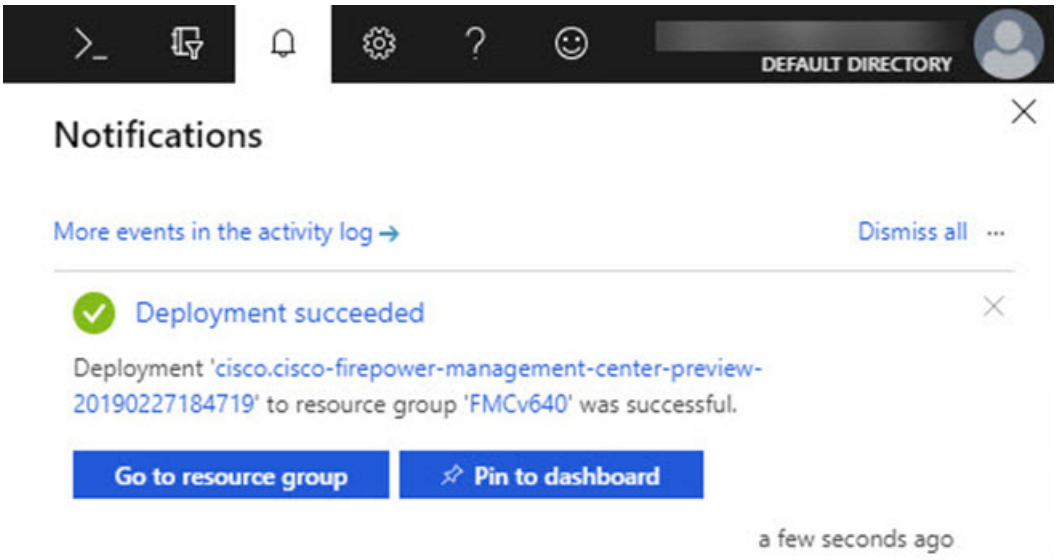
h) Click **OK**.

Step 6 View the configuration summary, and then click **OK**.

Step 7 View the terms of use and then click **Create**.

Step 8 Select **Notifications** (bell icon) at the top of the portal to view the status of the deployment.

Figure 1: Azure Notifications



From here, you can click on the deployment to see further details or go to the resource group once the deployment is successful. The total time until the Firewall Management Center Virtual is usable is approximately 30 minutes. Deployment times vary in Azure. Wait until Azure reports that the Firewall Management Center Virtual VM is running.

Step 9 (Optional) Azure provides a number of tools to help you monitor the state of your VM, including **Boot diagnostics** and **Serial console**. These tools allow you to see the state of your virtual machine as it boots up.

a) On the left menu, select **Virtual machines**.

b) Select your Firewall Management Center Virtual VM in the list. The overview page for the VM will open.

c) Scroll down to the **Support + troubleshooting** section and select **Boot diagnostics** or **Serial console**. A new pane with either the boot diagnostic **Screenshot** and **Serial log** or the text-based **Serial console** opens and starts the connection.

The readiness of the Firewall Management Center Virtual's Web interface is confirmed if you see the login prompt on either boot diagnostics or serial console.

Example:

```
Cisco Secure Firewall Management Center for Azure v7.6.0 (build 44)
FMCv76East login:
```

What to do next

- Verify that your Firewall Management Center Virtual deployment was successful. The Azure Dashboard lists the new Firewall Management Center Virtual VM under Resource Groups, along with all of the related resources (storage, network, route table, etc.).

Deploy from Azure Using a VHD and Resource Template

You can create your own custom Firewall Management Center Virtual images using a compressed VHD image available from Cisco. To deploy using a VHD image, you must upload the VHD image to your Azure storage account. Then, you can create a managed image using the uploaded disk image and an Azure Resource Manager template. Azure templates are JSON files that contain resource descriptions and parameter definitions.

Before you begin

- You need the JSON template and corresponding JSON parameter file for your Firewall Management Center Virtual template deployment. You can download these files from the GitHub repository.
- This procedure requires an existing Linux VM in Azure. We recommend that you use a temporary Linux VM (such as Ubuntu 16.04) to upload the compressed VHD image to Azure. This image will require about 50GB of storage when unzipped. Also, your upload time to Azure storage is faster from a Linux VM in Azure.

  If you need to create a VM, use one of the following methods:

  - Create a Linux virtual machine with the Azure CLI
  - Create a Linux virtual machine with the Azure portal

- In your Azure subscription, you should have a storage account available in the location in which you want to deploy the Firewall Management Center Virtual.

Procedure

Step 1 Download the Firewall Management Center Virtual compressed VHD image from the Cisco Download Software page:

a) Navigate to **Products** > **Security** > **Firewalls** > **Firewall Management** > **Secure Firewall Management Center Virtual**.

b) Click **Firepower Management Center Software**.

Follow the instructions for downloading the image.

For example, Cisco_Secure_FW_Mgmt_Center_Virtual_Azure-7.3.0-69.vhd.bz2

Step 2 Copy the compressed VHD image to your Linux VM in Azure.

There are many options that you can use to move files up to Azure and down from Azure. This example shows SCP or secure copy:

```
# scp /username@remotehost.com/dir/Cisco_Secure_FW_Mgmt_Center_Virtual_Azure-7.3.0-69.vhd.bz2
<linux-ip>
```

Step 3 Log in to the Linux VM in Azure and navigate to the directory where you copied the compressed VHD image.

Step 4 Unzip the Firewall Management Center Virtual VHD image.

There are many options that you can use to unzip or decompress files. This example shows the Bzip2 utility, but there are also Windows-based utilities that would work.

```
# bunzip2 Cisco_Secure_FW_Mgmt_Center_Virtual_Azure-7.3.0-69.vhd.bz2
```

Step 5 Upload the VHD to a container in your Azure storage account. You can use an existing storage account or create a new one. The storage account name can only contain lowercase letters and numbers.

There are many options that you can use to upload a VHD to your storage account, including AzCopy, Azure Storage Copy Blob API, Azure Storage Explorer, Azure CLI, or the Azure Portal. We do not recommend using the Azure Portal for a file as large as the Firewall Management Center Virtual VHD.

The following example shows the syntax using Azure CLI:

```
azure storage blob upload \
       --file <unzipped vhd> \
       --account-name <azure storage account> \
       --account-key yX7txxxxxxxx1dnQ== \
       --container <container> \
       --blob <desired vhd name in azure> \
       --blobtype page
```

Step 6 Create a Managed Image from the VHD:

a) In the Azure Portal, select **Images**.
b) Click **Add** to create a new image.
c) Provide the following information:

- **Subscription**—Choose a subscription from the drop-down list.
- **Resource group**—Choose an existing resource group or create a new one.
- **Name**—Enter a user-defined name for the managed image.
- **Region**—Choose the region in which the VM Is deployed.
- **OS type**—Choose **Linux** as the OS type.
- **VM generation**

  Choose **Generation 1** for BIOS boot mode.

  Choose **Generation 2** for UEFI boot mode.
- **Storage blob**—Browse to the storage account to select the uploaded VHD.
- **Account type**—As per your requirement, choose Standard HDD, Standard SSD, or Premium SSD, from the drop-down list.

  When you select the VM size planned for deployment of this image, ensure that the VM size supports the selected account type.

- **Host caching**—Choose Read/write from the drop-down list.
- **Data disks**—Leave at default; don't add a data disk.

d) Click **Create**.

Wait for the **Successfully created image** message under the **Notifications** tab.

Note Once the Managed Image has been created, the uploaded VHD and upload Storage Account can be removed.

Step 7 Acquire the Resource ID of the newly created Managed Image.

Internally, Azure associates every resource with a Resource ID. You'll need the Resource ID when you deploy new Firewall Management Center Virtual instances from this managed image.

a) In the Azure Portal, select **Images**.
b) Select the managed image created in the previous step.
c) Click **Overview** to view the image properties.
d) Copy the **Resource ID** to the clipboard.

The **Resource ID** takes the form of:

/subscriptions/<subscription-id>/resourceGroups/<resourceGroup>/providers/Microsoft.Compute/<container>/<vhdname>

Step 8 Build a Firewall Management Center Virtual instances using the managed image and a resource template:

a) On the Azure GUI, search for **Custom deployment**.
b) Under **Select a template**, click **Build your own template in the editor**.

You have a blank template that is available for customizing. See GitHub for the template files.

c) Paste your customized JSON template code into the window, and then click **Save**.
d) Choose a **Subscription** from the drop-down list.
e) Choose an existing **Resource group** or create a new one.
f) Choose a **Region** from the drop-down list.
g) Paste the Managed Image **Resource ID** from the previous step into the **Vm Image Id** field.
h) To deploy the Threat Defense Virtual without the diagnostic interface, enter a day-0 configuration script that includes the key-value pair **Diagnostic: OFF** in the Custom Data field. A sample day-0 configuration script is given below.

```
{
"AdminPassword": "E28@2OiUrhx!",
"Hostname": "ciscothreatdefensevirtual",
"FirewallMode": "routed",
"ManageLocally": "No",
"Diagnostic": "OFF"
}
```

Note The key value pair, "Diagnostic": "ON/OFF", is case-sensitive.

You can also modify the script in the Custom Data field in the ARM template that is used for fresh deployment.

Step 9 Click **Edit parameters** at the top of the **Custom deployment** page. You have a parameters template that is available for customizing.

a) Click **Load file** and browse to the customized Firewall Management Center Virtual parameter file. See GitHub for the template parameters.

b) Paste your customized JSON parameters code into the window, and then click **Save**.

Step 10 Review the Custom deployment details. Make sure that the information in **Basics** and **Settings** matches your expected deployment configuration, including the **Resource ID**.

Step 11 Review the Terms and Conditions, and check the **I agree to the terms and conditions stated above** check box.

Step 12 Click **Purchase** to deploy a Firewall Management Center Virtual instance using the managed image and a custom template.

If there are no conflicts in your template and parameter files, you should have a successful deployment.

The Managed Image is available for multiple deployments within the same subscription and region.

What to do next

- Update the Firewall Management Center Virtual's IP configuration in Azure.

Deploy the Azure Marketplace offers in the restricted Azure Private Marketplace environment

This applies only for the Azure Private Marketplace users. If you are using Azure Private Marketplace, then ensure that both Application Offers and required Virtual Machine Offers (hidden) are enabled for the user in respective private marketplace.

Virtual Machine Offers and Plans (hidden):

- Publisher ID: **cisco**
- Cisco Secure Firewall Management Center Virtual VM Offers (used for both the Cisco Secure Firewall Management Center Virtual Application offers)
  - Offer ID: **cisco-fmcv**
  - BYOL Plan ID: **fmcv-azure-byol**
- Cisco Firepower Management Center 300 Virtual
  - Offer ID: **cisco-fmcv300**
  - BYOL Plan ID: **fmcv300-azure-byol**

When user deploys the visible application offer from Marketplace, corresponding image from the VM offer plan is referenced and deployed.

Therefore, for the deployment to work, both Application and VM offers needs to be enabled/available on the Private Marketplace for the Azure tenant/subscription.

Refer the Azure documentation for enabling these application and VM offers in private marketplaces.

- Govern and control using private Azure Marketplace
- Add an offer to a private marketplace
- Set-AzMarketplacePrivateStoreOffer

Application offers are easily enabled via Azure UI as they are visible in the marketplace.

In order to enable hidden virtual machine offers in private marketplace, you might have to rely on CLI commands (at the time of this doc creation only CLI way is possible).

Sample command:

Cisco Secure Firewall Management Center Virtual BYOL plan can be enabled using similar sample command given below:

```
$Params = @{
  privateStoreId = '<private-store-id>'
  offerId = '<publisher-id>.<vm-offer-id>'
  SpecificPlanIdsLimitation =@('<plan-id-under-vm-offer>')
}
Set-AzMarketplacePrivateStoreOffer @Params

$Params = @{
  privateStoreId = '<private-store-id>'
  offerId = 'cisco.cisco-fmcv'
  SpecificPlanIdsLimitation =@('fmcv-azure-byol')
}
Set-AzMarketplacePrivateStoreOffer @Params
```

Note The sample command is only for reference, check Azure documentation for more details.

Reference Error message

```
{
  "code": "MarketplacePurchaseEligibilityFailed",
  "details": [
    {
      "code": "BadRequest",
     "message": "Offer with PublisherId: 'cisco', OfferId: 'cisco-XXXX' cannot be purchased
 due to validation errors. For more information see details.
Correlation Id: 'XXXXX`
This plan is not available for purchase because it needs to be added to your tenant's Private
 Marketplace. Contact your admin to request adding the plan.
Link to plan: <URL>.
Plan: '<PLAN NAME>'(planId=<VM-OFFER-PLAN-ID>),
Offer: <OFFER_NAME>, Publisher: 'Cisco Systems, Inc.'(publisherId='cisco').
…
…
    }
  ],
  "message": "Marketplace purchase eligibilty check returned errors. See inner errors for
details. "
}
```

User may run into the above error while deploying the Marketplace offer. To resolve this, both Application and VM offers need to be enabled/available on the Azure tenant/subscription.

Deploy the IPv6 Supported on Azure

Deploy the IPv6 Supported Secure Firewall Management Center Virtual on Azure

This chapter explains how to deploy the IPv6 Supported Firewall Management Center Virtual from the Azure portal.

About IPv6 Supported Deployment on Azure

Firewall Management Center Virtual offerings support both IPV4 and IPv6 from 7.3 and later. In Azure, you can deploy Firewall Management Center Virtual directly from the Marketplace offering, which creates or uses a virtual network, but currently, a limitation in Azure restricts the Marketplace application offer to use or create only IPv4-based VNet/subnets. Although, you can manually configure the IPv6 addresses to the existing VNet, a new Firewall Management Center Virtual instance cannot be added to the VNet configured with the IPv6 subnets. Azure imposes certain restrictions to deploy any third-party resources using an alternative approach other than deploying resources through Marketplace.

Cisco is currently offering two methods to deploy Firewall Management Center Virtual to support IPv6 addressing.

The following two distinct custom IPv6 templates are offered, where:

- **Custom IPv6 template (ARM template)** — It is offered to deploy Firewall Management Center Virtual with IPv6 configuration using an Azure Resource Manager (ARM) template that internally refers to a marketplace image on Azure. This template contains JSON files with resources and parameter definitions that you can configure to deploy IPv6-supported Firewall Management Center Virtual. To use this template, see Deploy from Azure using a Custom IPv6 Template with Marketplace Image References, on page 64.

  Programmatic deployment is a process of granting access to the VM images on Azure Marketplace to deploy custom templates through PowerShell, Azure CLI, ARM template, or API. You are restricted to deploy these custom templates on VM without providing access to VMs. If you attempt to deploy such custom templates on VM, then the following error message is displayed:

  Legal terms have not been accepted for this item on this subscription. To accept legal terms …..and configure programmatic deployment for the Marketplace item …..

  You can use one of the following methods to enable Programmatic deployment in Azure to deploy the custom IPv6 (ARM) template refering to the marketplace image:

  - **Azure Portal** – Enable programmatic deployment option corresponding to the Firewall Management Center Virtual offering available on Azure Marketplace for deploying the custom IPv6 template (ARM template).
  - **Azure CLI** – Run the CLI command to enable programmatic deployment for deploying the custom IPv6 (ARM template).

- **Custom VHD image and IPv6 template (ARM template)** — Create a managed image using the VHD image and ARM template on Azure. This process is similar to deploying Firewall Management Center Virtual by using a VHD and resource template. This template refers to a managed image during deployment

and uses an ARM template which you can upload and configure on Azure to deploy IPv6-supported Firewall Management Center Virtual. See, Deploy from Azure Using a VHD and Custom IPv6 Template, on page 69.

The process involved in deploying Firewall Management Center Virtual using custom IPv6 template (ARM template) in reference to marketplace image or VHD image with custom IPv6 template.

The steps involved in deploying the Firewall Management Center Virtual is as follows:

Table 11:

Step	Process
1	Create a Linux VM in Azure where you are planning to deploy the IPv6-supported Firewall Management Center Virtual
2	Enable Programmatic deployment option on Azure portal or Azure CLI **only** when you are deploying Firewall Management Center Virtual using the custom IPv6 template with Marketplace image reference.
3	Depending on the type of deployment download the following custom templates: • Custom IPv6 Template with Azure Marketplace reference image. VHD image with custom IPv6 (ARM) template.
4	Update the IPv6 parameters in the custom IPv6 (ARM) template. **Note** The equivalent Software image version parameter value of the marketplace image version is required only when you are deploying Firewall Management Center Virtual using the custom IPv6 template with Marketplace image reference. You must run a command to retrieve the Software version details.
5	Deploy the ARM template through Azure portal or Azure CLI.

Deploy from Azure using a Custom IPv6 Template with Marketplace Image References

The process involved in deploying Firewall Management Center Virtual using custom IPv6 template (ARM template) in reference to marketplace image.

Procedure

Step 1 Log into the Azure portal.

The Azure portal shows virtual elements associated with the current account and subscription regardless of data center location.

Step 2 Enable Programmatic deployment through Azure portal or Azure CLI as follows:

To enable this option on Azure Portal.

a) Under **Azure Services**, click **Subscriptions** to view the subscription blade page.

b) On the left pane, click **Programmatic Deployment** under the **Settings** option.

All the types of resources deployed on the VM are displayed along with the associated subscription offerings.

c) Click **Enable** under the **Status** column and corresponding to the Firewall Management Center Virtual offering to obtain for programmatic deployment of the custom IPv6 template.

OR

To enable this option through Azure CLI.

a) Go to the Linux VM/environment with Azure CLI installed and configured.
b) Run the following CLI command to enable programmatic deployment for deploying custom IPv6 (ARM) template.

You must accept the terms only once per subscription for each image.

 # Accept terms

az vm image terms accept -p <publisher> -f <offer> --plan <SKU/plan>

 # Verify that the terms were accepted (i.e., accepted=true)

az vm image terms show -p <publisher> -f <offer> --plan <SKU/plan>

Where,

- **<publisher>** - 'cisco'.
- **<offer>** - 'cisco-fmcv'
- **<sku/plan>** - 'fmcv-azure-byol'

The following is a command script example to enable programmatic deployment for deploying Firewall Management Center Virtual with BYOL subscription plan.

- **az vm image terms show -p cisco -f cisco-ftdv --plan fmcv-azure-byol**

Note PAYG deployments incur consumption-based Azure Marketplace charges and may be significantly more expensive than alternative licensing models. Use PAYG only when necessary and with caution. Before deployment, review the pricing and licensing terms, estimate expected costs, and obtain the appropriate budget approval.

Step 3 Run the following command to retrieve the Software version details equivalent to the marketplace image version.

az vm image list --all -p <publisher> -f <offer> -s <sku>

Where,

- **<publisher>** - 'cisco'.
- **<offer>** - 'cisco-fmcv'
- **<sku>** - 'fmcv-azure-byol'

The following is a command script example to retrieve the Software version details equivalent to the marketplace image version for Firewall Management Center Virtual.

az vm image list --all -p cisco -f cisco-fmcv -s fmcv-azure-byol

Step 4 Select one of the Firewall Management Center Virtual version from the list of available marketplace image versions that are displayed.

For IPv6 support deployment of Firewall Management Center Virtual, you must select the Firewall Management Center Virtual version as 73* or higher.

Step 5 Download the marketplace custom IPv6 template (ARM templates) from the Cisco GitHub repository.

Step 6 Prepare the parameters file by providing the deployment values in the parameters template file (JSON).

The following table describes the deployment values you need to enter in the custom IPv6 template parameters for Firewall Management Center Virtual custom deployment:

Parameter Name	Examples of allowed Values/Type	Description
vmName	cisco-fmcv	Name the Firewall Management Center Virtual VM in Azure.
softwareVersion	730.33.0	The software version of the marketplace image version.
billingType	BYOL	The licensing method is BYOL or PAYG. BYOL license is more cost effective compared to PAYG, hence it is recommended to opt for BYOL subscribed deployment.
adminUsername	hjohn	The username to log into Firewall Management Center Virtual. You cannot use the reserved name ‘admin’, which is assigned to administrator.
adminPassword	E28@4OiUrhx!	The admin password. Password combination must be an alphanumeric characters with 12 to 72 characters long. The password combination must comprise of lowercase and uppercase letters, numbers and special characters.
vmStorageAccount	hjohnvmsa	Your Azure storage account. You can use an existing storage account or create a new one. The storage account characters must be between three and 24 characters long. The password combination must contain only lowercase letters and numbers.
availabilityZone	0	Specify the availability zone for deployment, public IP and the virtual machine will be created in the specified availability zone. Set it to '**0**' if you do not need availability zone configuration. Ensure that selected region supports availability zones and value provided is correct. (This must be an integer between 0-3).

Parameter Name	Examples of allowed Values/Type	Description
ipAllocationMethod	Dynamic	IP allocation from Azure. Static : Manual, Dynamic : DHCP
mgmtSubnetName	mgmt	Management center IP on the mgmt interface (example: 192.168.0.10)
mgmtSubnetIP	10.4.1.15	FMC IP on the mgmt interface (example: 192.168.0.10)
mgmtSubnetIPv6	ace:cab:deca:dddd::c3	FMC IPv6 on the mgmt interface (example: ace:cab:deca:dddd::6)
customData	`{\"AdminPassword\": \"E28@4OiUrhx!\",\"Hostname\": \"cisco-mcv\", \"IPv6Mode\"`	The field to provide in the Day 0 configuration to the Firewall Management Center Virtual. By default it has the following three key-value pairs to configure: • 'admin' user password • Firewall Management Center Virtual hostname • the Firewall Management Center Virtual hostname or CSF-DM for management. 'ManageLocally : yes' - This configures the CSF-DM to be used as Firewall Threat Defense Virtual manager. You can configure the Firewall Management Center Virtual as Firewall Threat Defense Virtual manager and also give the inputs for fields required to configure the same on Firewall Management Center Virtual.
virtualNetworkResourceGroup	cisco-mcv-rg	Name of the resource group containing the virtual network. In case virtualNetworkNewOr Existing is new, this value should be same as resource group selected for template deployment.
virtualNetworkName	cisco-mcv-vnet	The name of the virtual network.
virtualNetworkNewOrExisting	new	This parameter determines whether a new virtual network should be created or an existing virtual network is to be used.
virtualNetworkAddressPrefixes	10.151.0.0/16	IPv4 address prefix for the virtual network, this is required only if 'virtualNetworkNewOrExisting' is set to 'new'.
virtualNetworkv6AddressPrefixes	ace:cab:deca::/48	IPv6 address prefix for the virtual network, this is required only if 'virtualNetworkNewOrExisting' is set to 'new'.

Parameter Name	Examples of allowed Values/Type	Description
Subnet1Name	mgmt	Management subnet name.
Subnet1Prefix	10.151.1.0/24	Management subnet IPv4 Prefix, this is required only if 'virtualNetworkNewOrExisting' is set to 'new'.
Subnet1IPv6Prefix	ace:cab:deca:1111::/64	Management subnet IPv6 Prefix, this is required only if 'virtualNetworkNewOrExisting' is set to 'new'.
subnet1StartAddress	10.151.1.4	Management interface IPv4 address.
subnet1v6StartAddress	ace:cab:deca:1111::6	Management interface IPv6 address.
Subnet2Name	diag	Data interface 1 subnet name.
Subnet2Prefix	10.151.2.0/24	Data interface 1 Subnet IPv4 prefix, this is required only if 'virtualNetworkNewOrExisting' is set to 'new'.
Subnet2IPv6Prefix	ace:cab:deca:2222::/64	Data interface 1 Subnet IPv6 Prefix, this is required only if 'virtualNetworkNewOrExisting' is set to 'new'.
subnet2StartAddress	10.151.2.4	Data interface 1 IPv4 address.
subnet2v6StartAddress	ace:cab:deca:2222::6	Data interface 1 IPv6 address.
Subnet3Name	inside	Data interface 2 subnet name.
Subnet3Prefix	10.151.3.0/24	Data interface 2 Subnet IPv4 Prefix, this is required only if 'virtualNetworkNewOrExisting' is set to 'new'.
Subnet3IPv6Prefix	ace:cab:deca:3333::/64	Data interface 2 Subnet IPv6 Prefix, this is required only if 'virtualNetworkNewOrExisting' is set to 'new'.
subnet3StartAddress	10.151.3.4	Data interface 2 IPv4 address.
subnet3v6StartAddress	ace:cab:deca:3333::6	Data interface 2 IPv6 address.
Subnet4Name	outside	Data interface 3 subnet name.
Subnet4Prefix	10.151.4.0/24	Data interface 3 subnet IPv4 Prefix, this is required only if 'virtualNetworkNewOrExisting' is set to 'new'
Subnet4IPv6Prefix	ace:cab:deca:4444::/64	Data interface 3 Subnet IPv6 Prefix, this is required only if 'virtualNetworkNewOrExisting' is set to 'new'.
subnet4StartAddress	10.151.4.4	Data interface 3 IPv4 Address.

Parameter Name	Examples of allowed Values/Type	Description
subnet4v6StartAddress	ace:cab:deca:4444::6	Data interface 3 IPv6 Address.
vmSize	Standard_D4_v2	Size of the Firewall Management Center Virtual VM. Standard_D4_v2 is the default.

Step 7 Use the ARM template to deploy Firewall Management Center Virtual firewall through the Azure portal or Azure CLI. For information about deploying the ARM template on Azure, refer to the following Azure documentation:

- Create and deploy ARM templates by using the Azure portal
- Deploy a local ARM template through CLI

What to do next

Your next steps depend on what management mode you chose.

- If you chose **No** for **Enable Local Manager**, you'll use the Secure Firewall Management Center to manage your Firewall Threat Defense Virtual; see Managing the Secure Firewall Threat Defense Virtual with the Secure Firewall Management Center.
- If you chose **Yes** for **Enable Local Manager**, you'll use the integrated Secure Firewall Device Manager to manage your ; see Managing the Secure Firewall Threat Defense Virtual with the Secure Firewall device manager.

  See How to Manage Your Secure Firewall Threat Defense Virtual Device for an overview of how to choose your management option.

Verify that your management center virtual deployment was successful. The Azure Dashboard lists the new management center virtual VM under Resource Groups, along with all of the related resources (storage, network, route table, etc.).

Deploy from Azure Using a VHD and Custom IPv6 Template

You can create your own custom Firewall Management Center Virtual images using a compressed VHD image available from Cisco. This process is similar to deploying Firewall Management Center Virtual by using a VHD and resource template.

Before you begin

- You need the JSON template and corresponding JSON parameter file for your Firewall Management Center Virtual deployment using VHD and ARM updated template on Github, where you'll find instructions on how to build a template and parameter file.
- This procedure requires an existing Linux VM in Azure. We recommended you use a temporary Linux VM (such as Ubuntu 16.04) to upload the compressed VHD image to Azure. This image will require about 50GB of storage when unzipped. Also, your upload times to Azure storage will be faster from a Linux VM in Azure.

  If you need to create a VM, use one of the following methods:

- Create a Linux virtual machine with the Azure CLI
- Create a Linux virtual machine with the Azure portal

- In your Azure subscription, you should have a storage account available in the Location in which you want to deploy the Firewall Management Center Virtual.

Procedure

Step 1 Download the Firewall Management Center Virtual compressed VHD image (*.bz2) from the Cisco Download Software page:

a) Navigate to **Products** > **Security** > **Firewalls** > **Firewall Management** > **Secure Firewall Management Center Virtual**.

b) Click **Firepower Management Center Software**.

Follow the instructions for downloading the image.

Cisco_Secure_Firewall_Threat_Defense_Virtual-X.X.X-xxx.vhd.bz2

For example, Cisco_Secure_FW_Mgmt_Center_Virtual_Azure-7.3.0-69.vhd.bz2

Step 2 Perform the deployment steps provided in the Deploy from Azure Using a VHD and Resource Template.

Step 3 Click **Edit parameters** at the top of the **Custom deployment** page. You have a parameters template that is available for customizing.

a) Click **Load** file and browse to the customized Firewall Management Center Virtual parameter file. See the sample for the Azure Firewall Management Center Virtual deployment using VHD and custom IPv6 (ARM) template on Github, where you'll find instructions on how to build a template and parameter file.

b) Paste your customized JSON parameters code into the window, and then click **Save**.

The following table describes the deployment values you need to enter in the custom IPv6 template parameters for Firewall Management Center Virtual deployment:

Parameter Name	Examples of allowed values/types	Description
vmName	cisco-fmcv	Name the Firewall Management Center Virtual VM in Azure.
vmImageId	/subscriptions/{subscription-id}/resourceGroups/{resource-group-name}/providers/Microsoft.Compute/images/{image-name}	The ID of the image used for deployment. Internally, Azure associates every resource with a Resource ID.
adminUsername	hjohn	The username to log into Firewall Management Center Virtual. You cannot use the reserved name 'admin', which is assigned to administrator.
adminPassword	E28@4OiUrhx!	The admin password.

Parameter Name	Examples of allowed values/types	Description
		Password combination must be an alphanumeric characters with 12 to 72 characters long. The password combination must comprise of lowercase and uppercase letters, numbers and special characters.
vmStorageAccount	hjohnvmsa	Your Azure storage account. You can use an existing storage account or create a new one. The storage account characters must be between three and 24 characters long. The password combination must contain only lowercase letters and numbers.
availabilityZone	0	Specify the availability zone for deployment, public IP and the virtual machine will be created in the specified availability zone. Set it to '**0**' if you do not need availability zone configuration. Ensure that selected region supports availability zones and value provided is correct. (This must be an integer between 0-3).
customData	`{\"AdminPassword\": \"E28@4OiUrhx\",\"Hostname\": \"cisco-mcv\", \"IPv6Mode\": \"DHCP\"}`	The field to provide in the Day 0 configuration to the Firewall Management Center Virtual. By default it has the following three key-value pairs to configure: • 'admin' user password • CSF-MCv hostname • the CSF-MCv hostname or CSF-DM for management. 'ManageLocally : yes' - This configures the CSF-DM to be used as Firewall Threat Defense Virtual manager. You can configure the CSF-MCv as Firewall Threat Defense Virtual manager and also give the inputs for fields required to configure the same on CSF-MCv.
virtualNetworkResourceGroup	cisco-fmcv	Name of the resource group containing the virtual network. In case virtualNetworkNewOr Existing is new,

Parameter Name	Examples of allowed values/types	Description
		this value should be same as resource group selected for template deployment.
virtualNetworkName	cisco-mcv-vnet	The name of the virtual network.
ipAllocationMethod	Dynamic	IP allocation from Azure. Static : Manual, Dynamic : DHCP
mgmtSubnetName	mgmt	Management center IP on the mgmt interface (example: 192.168.0.10)
mgmtSubnetIP	10.4.1.15	FMC IP on the mgmt interface (example: 192.168.0.10)
mgmtSubnetIPv6	ace:cab:deca:dddd::c3	FMC IPv6 on the mgmt interface (example: ace:cab:deca:dddd::6)
virtualNetworkNewOrExisting	new	This parameter determines whether a new virtual network should be created or an existing virtual network is to be used.
virtualNetworkAddressPrefixes	10.151.0.0/16	IPv4 address prefix for the virtual network, this is required only if 'virtualNetworkNewOr Existing' is set to 'new'.
virtualNetworkv6AddressPrefixes	ace:cab:deca::/48	IPv6 address prefix for the virtual network, this is required only if 'virtualNetworkNewOr Existing' is set to 'new'.
Subnet1Name	mgmt-ipv6	Management subnet name.
Subnet1Prefix	10.151.1.0/24	Management subnet IPv4 Prefix, this is required only if 'virtualNetworkNewOr Existing' is set to 'new'.
Subnet1IPv6Prefix	ace:cab:deca:1111::/64	Management subnet IPv6 Prefix, this is required only if 'virtualNetworkNewOr Existing' is set to 'new'.
subnet1StartAddress	10.151.1.4	Management interface IPv4 address.
subnet1v6StartAddress	ace:cab:deca:1111::6	Management interface IPv6 address.
Subnet2Name	diag	Data interface 1 subnet name.
Subnet2Prefix	10.151.2.0/24	Data interface 1 Subnet IPv4 prefix, this is required only if

Parameter Name	Examples of allowed values/types	Description
		'virtualNetworkNewOr Existing' is set to 'new'.
Subnet2IPv6Prefix	ace:cab:deca:2222::/64	Data interface 1 Subnet IPv6 Prefix, this is required only if 'virtualNetworkNewOr Existing' is set to 'new'.
subnet2StartAddress	10.151.2.4	Data interface 1 IPv4 address.
subnet2v6StartAddress	ace:cab:deca:2222::6	Data interface 1 IPv6 address.
Subnet3Name	inside	Data interface 2 subnet name.
Subnet3Prefix	10.151.3.0/24	Data interface 2 Subnet IPv4 Prefix, this is required only if 'virtualNetworkNewOr Existing' is set to 'new'.
Subnet3IPv6Prefix	ace:cab:deca:3333::/64	Data interface 2 Subnet IPv6 Prefix, this is required only if 'virtualNetworkNewOr Existing' is set to 'new'.
subnet3StartAddress	10.151.3.4	Data interface 2 IPv4 address.
subnet3v6StartAddress	ace:cab:deca:3333::6	Data interface 2 IPv6 address.
Subnet4Name	outside	Data interface 3 subnet name.
Subnet4Prefix	10.151.4.0/24	Data interface 3 subnet IPv4 Prefix, this is required only if 'virtualNetworkNewOr Existing' is set to 'new'
Subnet4IPv6Prefix	ace:cab:deca:4444::/64	Data interface 3 Subnet IPv6 Prefix, this is required only if 'virtualNetworkNewOr Existing' is set to 'new'.
subnet4StartAddress	10.151.4.4	Data interface 3 IPv4 Address.
subnet4v6StartAddress	ace:cab:deca:4444::6	Data interface 3 IPv6 Address.
vmSize	Standard_D4_v2	Size of the Firewall Management Center Virtual VM. Standard_D4_v2 is the default.

Step 4 Use the ARM template to deploy Firewall Management Center Virtual firewall through the Azure portal or Azure CLI. For information about deploying the ARM template on Azure, refer to the following Azure documentation:

- Create and deploy ARM templates by using the Azure portal

- Deploy a local ARM template through CLI

What to do next

Verify the Firewall Management Center Virtual Deployment

After the Firewall Management Center Virtual VM is created, the Microsoft Azure Dashboard lists the new Firewall Management Center Virtual VM under Resource groups. The corresponding storage account and network resources also are created and listed. The Dashboard provides a unified view of your Azure assets, and provides an easy, at-a-glance assessment of the health and performance of the Firewall Management Center Virtual.

Before you begin

The Firewall Management Center Virtual VM is started automatically. During deployment the status is listed as "Creating" while Azure creates the VM, and then the status changes to "Running" once the deployment is complete.

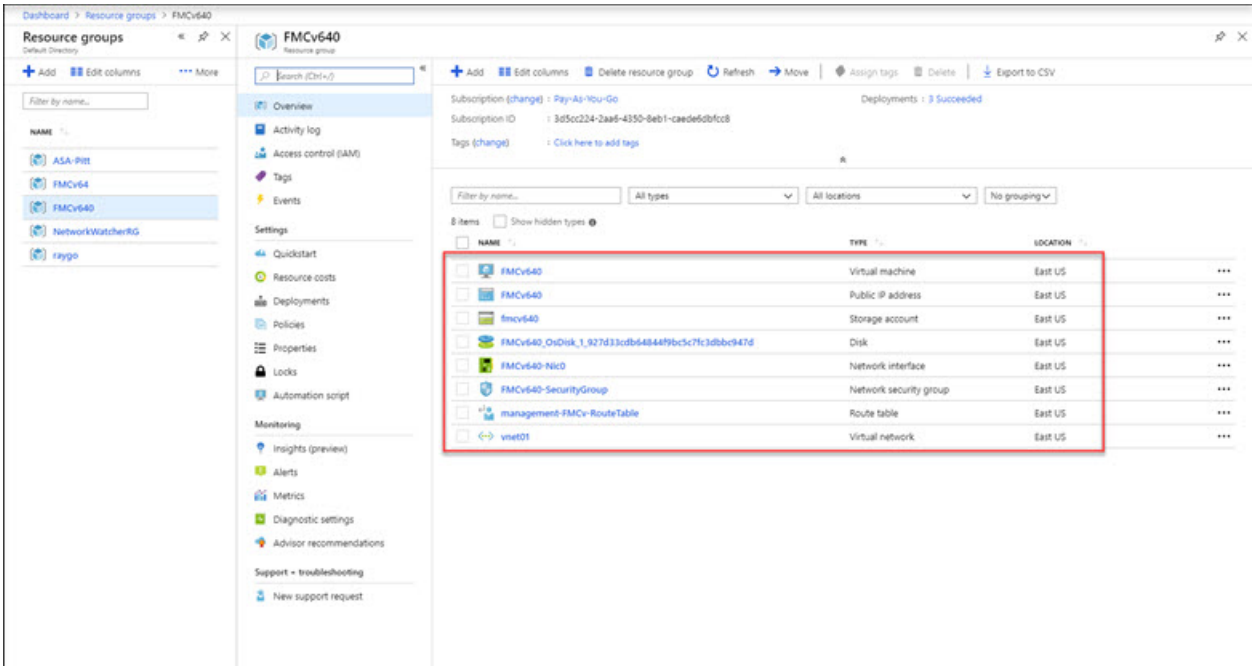
Note Remember that deployment times vary in Azure, and the total time until the Firewall Management Center Virtual is usable is approximately 30 minutes, even when the Azure Dashboard shows the status of the Firewall Management Center Virtual VM as "Running".

Procedure

Step 1 To view the Firewall Management Center Virtual resource group and its resources after deployment is completed, from the left menu pane, click **Resource groups** to access the Resource groups page.

The following figure shows an example of a Resources groups page in the Microsoft Azure portal. Notice the Firewall Management Center Virtual VM as well as its corresponding resources (storage account, network resources, etc.).

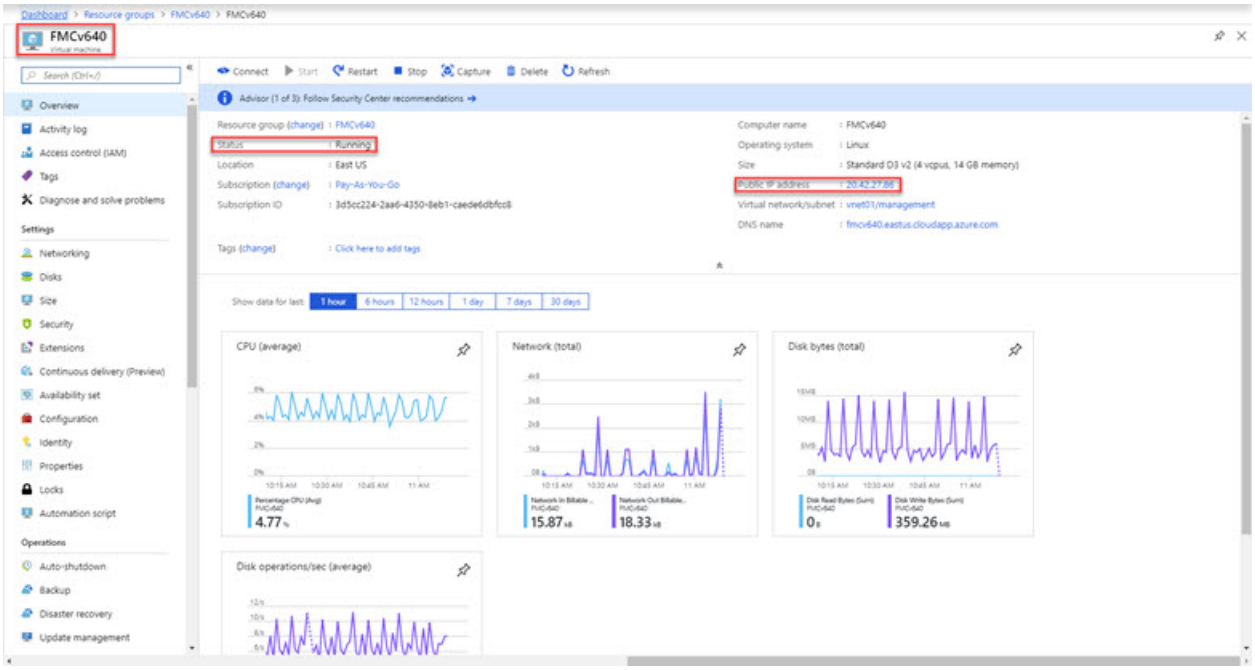
Figure 2: Azure Firewall Management Center Virtual Resource Group Page



Step 2 To view details of the Firewall Management Center Virtual VM associated with the resource group, click the name of the Firewall Management Center Virtual VM.

The following figure shows an example of the **Virtual machine** overview page associated with the Firewall Management Center Virtual VM. You access this overview from the Resources groups page.

Figure 3: Virtual Machine Overview



Observe that the status is Running. You can stop, start, restart, and delete the Firewall Management Center Virtual VM from the **Virtual machine** page in the Microsoft Azure portal. Note that these controls are not graceful shutdown mechanisms for the Firewall Management Center Virtual; see Guidelines and Limitations, on page 51 for graceful shutdown information.

Step 3 From the **Virtual machine** page, find the **Public IP address** assigned to the Firewall Management Center Virtual.



Note You can hover over the IP address and select **Click to copy** to copy the IP address.

Step 4 Direct your browser to **https://***public_ip/*, where *public_ip* is the IP address assigned to the Firewall Management Center Virtual's management interface when you deployed the VM.

The login page appears.

Step 5 Log in using **admin** as the username and the password for the admin account that you specified when you deployed the VM.

What to do next

- We recommend that you complete some administrative tasks that make your deployment easier to manage, such as creating users and reviewing health and system policies. Refer to Firewall Management Center Virtual Initial Administration and Configuration, on page 147 for an overview how to get started.
- You should also review your device registration and licensing requirements.
- For information on how you can begin to configure your system, see the complete Secure Firewall Management Center Configuration Guide for your software version.

Monitoring and Troubleshooting

This section includes general monitoring and troubleshooting guidelines for the Firewall Management Center Virtual appliance deployed in Micosoft Azure. Monitoring and troubleshooting can relate to either the deployment of the VM in Azure, or the Firewall Management Center Virtual appliance itself.

Azure Monitoring of the VM Deployment

Azure provides a number of tools under the **Support + troubleshooting** menu that provide quick access to tools and resources to help you diagnose and resolve issues and receive additional assistance. Two items of interest include:

- **Boot diagnostics**—Allows you to see the state of your Firewall Management Center Virtual VM as it boots up. The boot diagnostics collects serial log information from the VM as well as screen shots. This can help you to diagnose any startup issues.
- **Serial console**—The VM serial console in the Azure portal provides access to a text-based console. This serial connection connects to the COM1 serial port of the virtual machine, providing serial and SSH access to the Firewall Management Center Virtual's command line interface using the public IP address assigned to the Firewall Management Center Virtual.

Firewall Management Center Virtual Monitoring and Logging

Troubleshoots and general logging operatations follow the same procedures as current Firewall Management Center and Firewall Management Center Virtual models. Refer to the *System Monitoring and Troubleshooting* section of the Secure Firewall Management Center Configuration Guide for your version.

In addition, the Microsoft Azure Linux Agent (waagent) manages Linux provisioning and VM interaction with the Azure Fabric Controller. As such, the following are important logs for troubleshooting:

- **/var/log/waagent.log**—This log will have any errors from the Firewall Management Center provisioning with Azure.
- **/var/log/firstboot.S07install_waagent**—This log will have any errors from the waagent installation.

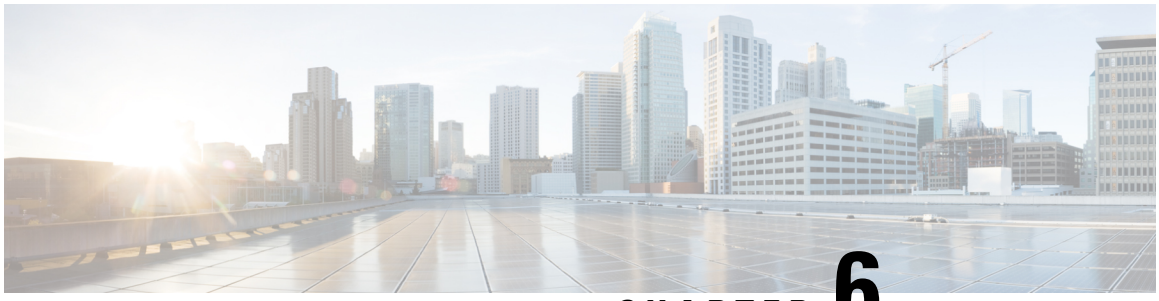
Azure Provisioning Failures

Provisioning errors using the Azure Marketplace solution template are uncommon. However, should you encounter a provisioning error, keep the following points in mind:

- Azure has a 20 minute timeout for the virtual machine to provision with the waagent, at which point it is rebooted.
- If the Firewall Management Center has trouble provisioning for any reason, the 20 minute timer tends to end in the middle of the Firewall Management Center database initialization, likely resulting in a deployment failure.
- If the Firewall Management Center fails to provision in 20 minutes, we recommend that you start over.
- You can consult the */var/log/waagent.log* for troubleshooting information.
- If you see HTTP connection errors in the serial console, this suggests that the waagent cannot communicate with the fabric. You should review your network settings upon redeploy.

Feature History

Feature Name	Releases	Feature Information
High Availability (HA) Support	7.4.2	Firewall Management Center Virtual High Avail is supported on the following models: FMCv10, FMCv300.
FMCv300 support	7.4.2	FMCv300 is supported.
Deploy the Firewall Management Center Virtual on the Microsoft Azure public cloud.	6.4.0	Initial support.



CHAPTER 6

Deploy the Firewall Management Center Virtual on GCP

Google Cloud Platform (GCP) is a public cloud service provided by Google that that allows you to build and host applications Google's scalable infrastructure. Google's virtual private cloud (VPC) gives you the flexibility to scale and control how workloads connect regionally and globally. GCP allows you to build your own VPCs on top of Google's public infrastructure.

You can deploy the Firewall Management Center Virtual on the GCP.

- Overview, on page 79
- Prerequisites, on page 80
- Guidelines and Limitations, on page 81
- Sample Network Topology, on page 81
- Deploy the Firewall Management Center Virtual, on page 82
- Access the Firewall Management Center Virtual Instance on GCP, on page 85

Overview

The Firewall Management Center Virtual runs the same software as the physical Firewall Management Center to deliver proven security functionality in a virtual form factor. The Firewall Management Center Virtual can be deployed in the public GCP. It can then be configured to manage virtual and physical devices.

GCP Machine Type Support

The Firewall Management Center Virtual supports both compute-optimized and general purpose machine high-memory machine types, and high-CPU machine types. The Firewall Management Center Virtual supports the following GCP machine types.

Note Supported machine types may change without notice.

Note Machine type selection is restricted. The user can choose only machine types that are supported for the specific Firewall Management Center Virtual version selected.

Table 12: Supported Compute-Optimized Machine Types

Compute-Optimized Machine Types	Attributes	
	vCPUs	RAM (GB)
c2d-standard-8	8	32 GB
c2d-standard-16	16	64 GB

Table 13: Supported General Purpose Machine Types

General Purpose Machine Types	Attributes	
	vCPUs	RAM (GB)
e2-standard-8	8	32
e2-standard-16	16	64
e2-highmem-8	8	64
e2-highmem-16	16	128
n1-highmem-8	8	52
n1-highmem-16	16	104
n2d-standard-8	8	32
n2d-standard-16	16	64
t2d-standard-8 (version 10.1.0 and later)	8	32
t2d-standard-16 (version 10.1.0 and later)	16	64
n2d-standard-8 (version 10.1.0 and later)	8	32
n2d-standard-16 (version 10.1.0 and later)	16	64

Prerequisites

- Create an GCP account at https://cloud.google.com.
- A Cisco Smart Account. You can create one at Cisco Software Central (https://software.cisco.com/).
  - Configure all license entitlements for the security services from the Firewall Management Center.
  - See “Licensing the System” in the Firewall Management Center Configuration Guide for more information about how to manage licenses.

- Interface requirements:
  - Management interface — One used to connect the Firewall Threat Defense device to the Firewall Management Center.
- Communications paths:
  - Public IP for administrative access to the Firewall Management Center.
- For the Firewall Management Center Virtual and System compatibility, see Cisco Secure Firewall Threat Defense Compatibility Guide.

Guidelines and Limitations

Supported Features

- Deployment in the GCP Compute Engine
- Maximum of 32 vCPUs per instance (based on the GCP machine type)
- Licensing – Only BYOL is supported

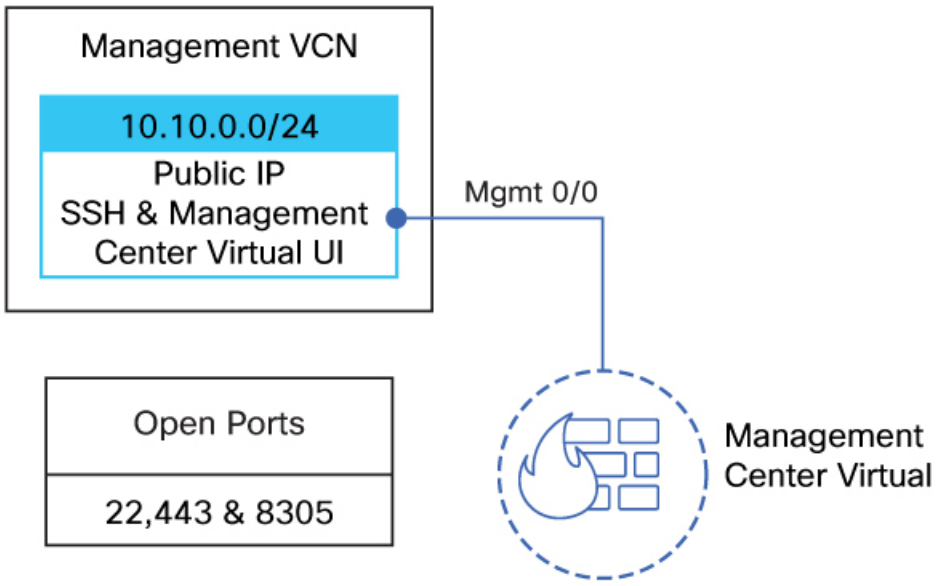
Unsupported Features

- IPv6
- Firewall Management Center Virtual native HA
- Autoscale
- Transparent/inline/passive modes
- Multi-context mode

Sample Network Topology

The following figure illustrates the typical topology for the Firewall Management Center Virtual with 1 subnet configured in GCP.

Figure 4: Topology Example for theFirewall Management Center Virtual Deployment on GCP



Deploy the Firewall Management Center Virtual

The following procedures describe how to prepare your GCP environment and launch the Firewall Management Center Virtual instance.

Create VPC Networks

The Firewall Management Center Virtual deployment requires the Management VPC for the management Firewall Management Center Virtual. See Figure 1 on page 3 as a guide.

Procedure

Step 1 In the GCP console, choose **VPC networks**, then click **Create VPC Network**.

Step 2 In the **Name** field, enter a descriptive name for your VPC network.

Step 3 From **Subnet creation mode**, click **Custom**.

Step 4 In the **Name** field under **New subnet**, enter the desired name.

Step 5 From the **Region** drop-down list, select the region appropriate for your deployment.

Step 6 From the **IP address range field**, enter the first network's subnet in CIDR format, such as 10.10.0.0/24.

Step 7 Accept the defaults for all other settings, then click **Create**.

Create the Firewall Rules

Each of the VPC networks requires firewall rules to allow SSH and traffic. Create the firewall rules for each VPC network.

Procedure

Step 1 In the GCP console, choose **Networking** > **VPC network** > **Firewall**, then click **Create Firewall Rule**.

Step 2 In the **Name** field, enter a descriptive name for your firewall rule, for example, *vpc-asiasouth-mgmt-ssh*.

Step 3 From the **Network** drop-down list, select the name of the VPC network for which you are creating the firewall rule, for example, *fmcv-south-mgmt*.

Step 4 From the **Targets** drop-down list, select the option applicable for your firewall rule, for example, **All instances in the network**.

Step 5 In the **Source IP ranges** field, enter the source IP address ranges in CIDR format, for example, 0.0.0.0/0.

Traffic is only allowed from sources within these IP address ranges.

Step 6 Under **Protocols and ports**, select **Specified protocols and ports**.

Step 7 Add your security rules:

a) Add a rule to allow SSH (TCP/22).
b) Add a rule to allow TCP port 443.

You access the Firewall Management Center Virtual UI which requires port 443 to be opened for HTTPS connections.

Step 8 Click **Create**.

Create the Firewall Management Center Virtual Instance on GCP

You can follow the steps below to deploy the Firewall Management Center Virtual instance from the GCP console.

Procedure

Step 1 Log into to the GCP Console.

Step 2 Click **Navigation menu** > **Marketplace**.

Step 3 Search the Marketplace for “Firewall Management Center BYOL” and choose the offering.

Step 4 Click **Launch**.

a) **Deployment name** — Specify a unique name for the instance.
b) **Image version** — Select the version from the drop-down list.
c) **Zone** — Select the zone where you want to deploy the Firewall Management Center Virtual.
d) **Machine type** — Choose the correct machine type based on the GCP Machine Type Support, on page 79.
e) **SSH key (optional)** — Paste the public key from the SSH key pair.

The key pair consists of a public key that GCP stores and a private key file that the user stores. Together they allow you to connect to your instance securely. Be sure to save the key pair to a known location, as it will be required to connect to the instance.

f) Choose whether to allow or **Block project-wide SSH keys** to access this instance. See the Google documentation Allowing or blocking project-wide public SSH keys from a Linux instance.

g) **Startup script** — Provide the day0 configuration for the Firewall Management Center Virtual.

The following example shows a sample day0 configuration you can copy and paste in the **Startup script** field:

```
{
"AdminPassword": "myPassword@123456",
"Hostname": "cisco-fmcv"
}
```

Tip To prevent execution errors, you should validate your day0 configuration using a JSON validator.

h) Select the **Boot disk type** from the drop-down list.

By default, the **Standard Persistent Disk** is selected. Cisco recommends that you use the default Boot disk type.

i) The **Boot disk size in GB** default value is 250 GB. Cisco recommends that you keep the default boot disk size. It cannot be less than 250 GB.

j) Click **Add network interface** to configure the Management interface.

Note You cannot add interfaces to an instance after you create it. If you create the instance with an improper interface configuration, you must delete the instance and recreate it with the proper interface configuration.

- From the **Network** drop-down list, select a VPC network, for example, *vpc-branch-mgmt*.
- From the **External IP** drop-down list, select the appropriate option.

  For the management interface, select the **External IP** to **Ephemeral**.
- Click **Done**.

k) **Firewall**— Apply the firewall rules.

- Check the **Allow TCP port 22 traffic from the Internet (SSH access)** check box to allow SSH.
- Check the **Allow HTTPS traffic from the Internet (FMC GUI)** check box to allow HTTPS connections.
- Check the **Allow TCP port 8305 traffic from the Internet (SFTunnel comm.)** check box to allow the Firewall Management Center Virtual and managed devices to communicate using a two-way, SSL-encrypted communication channel.

l) Click **More** to expand the view and make sure that **IP Forwarding** is set to **On**.

Step 5 Click **Deploy**.

Note Startup time depends on a number of factors, including resource availability. It can take up to 35 minutes for the initialization to complete. Do not interrupt the initialization or you may have to delete the appliance and start over.

What to do next

View the instance details from the VM instance page of the GCP console. You'll find the internal IP address, external IP address, and controls to stop and start the instance. You need to stop the instance if you need to edit it.

Access the Firewall Management Center Virtual Instance on GCP

Make sure that you have already created a firewall rule to allow SSH (TCP connections through port 22); for more information, refer to Create the Firewall Rules.

This firewall rule enables access to the Firewall Management Center Virtual instance and allows you to connect to the instance using the following methods.

- External IP
  - Browser window
  - Any other SSH client or third-party tools
- Serial console
  - Gcloud command line

See the Google documentation, Connecting to instances for more information.

Note If you choose not to add a Day0 configuration, you can log in to the Firewall Management Center Virtual instance using the default credentials. You are prompted to set the password on the first login attempt.

Connect to the Firewall Management Center Virtual Instance Using the Serial Console

Procedure

Step 1 In the GCP console, choose **Compute Engine** > **VM instances**.

Step 2 Click the Firewall Management Center Virtual instance name to open the **VM instance details** page.

Step 3 Under the **Details** tab, click **Connect to serial console**.

See the Google documentation, Interacting with the serial console for more information.

Connect to the Firewall Management Center Virtual Instance Using an External IP

The Firewall Management Center Virtual instance is assigned with an internal IP and an external IP. You can use the external IP to access the Firewall Management Center Virtual instance.

Procedure

Step 1 In the GCP console, choose **Compute Engine** > **VM instances**.

Step 2 Click the Firewall Management Center Virtual instance name to open the VM instance details page.

Step 3 Under the **Details** tab, click the drop-down menu for the **SSH** field.

Step 4 Select the desired option from the **SSH** drop-down menu.

You can connect to the Firewall Management Center Virtual instance using the following method.

- Any other SSH client or third-party tools—See the Google documentation, Connecting using third-party tools for more information.

Connect to the Firewall Management Center Virtual Instance Using Gcloud

Procedure

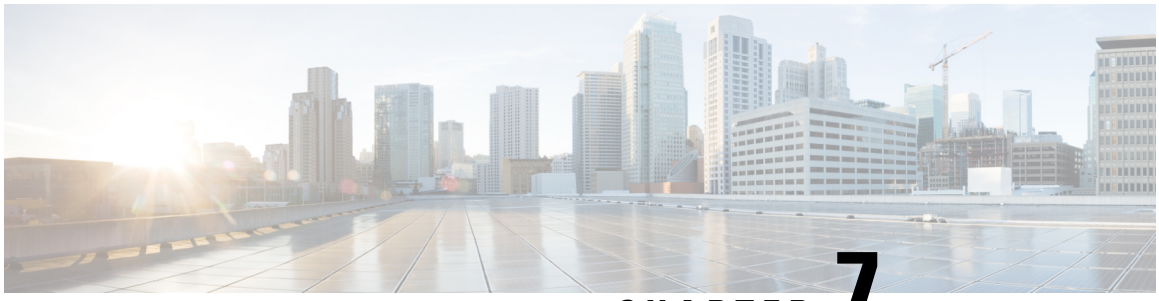
Step 1 In the GCP console, choose **Compute Engine** > **VM instances**.

Step 2 Click the Firewall Management Center Virtual instance name to open the **VM instance details** page.

Step 3 Under the **Details** tab, click the drop-down menu for the **SSH** field.

Step 4 Click **View gcloud command** > **Run in Cloud Shell**.

The Cloud Shell terminal window opens. See the Google documentation, gcloud command-line tool overview, and gcloud compute ssh for more information.



CHAPTER 7

Deploy the Firewall Management Center Virtual on OCI

Oracle Cloud Infrastructure (OCI) is a public cloud computing service that enables you to run your applications in a highly available, hosted environment offered by Oracle. OCI provides real-time elasticity for enterprise applications by combining Oracle's autonomous services, integrated security, and serverless compute.

You can deploy the Firewall Management Center Virtual on OCI.

- Overview, on page 89
- Prerequisites, on page 91
- Guidelines and Limitations, on page 91
- Sample Network Topology, on page 91
- Deploy the Firewall Management Center Virtual, on page 92
- Access the Firewall Management Center Virtual Instance on OCI, on page 96

Overview

The Firewall Management Center Virtual runs the same software as physical Firewall Management Center to deliver proven security functionality in a virtual form factor. The Firewall Management Center Virtual can be deployed in the public OCI. It can then be configured to manage virtual and physical devices.

OCI Compute Shapes

A shape is a template that determines the number of CPUs, amount of memory, and other resources that are allocated to an instance. The Firewall Management Center Virtual support the following OCI shape types:

Table 14: Supported Compute Shapes for Firewall Management Center Virtual

OCI Shape	Supported Firewall Management Center Virtual version	Attributes	
		oCPUs	RAM (GB)
Intel VM.StandardB1.4	7.3.0 and later	4	48
Intel VM.Standard2.4	7.1.0 and later	4	60
Intel VM.Standard3.Flex	7.3.0 and later	4	32

OCI Shape	Supported Firewall Management Center Virtual version	Attributes	
		oCPUs	RAM (GB)
Intel VM.Optimized3.Flex	7.3.0 and later	4	32
AMD VM.Standard.E4.Flex	7.3.0 and later	4	32
AMD VM.Standard.E5.Flex	7.6.4 and later 7.6.x releases, 10.1.0 and later	4	32
AMD VM.Standard.E6.Flex	7.6.4 and later 7.6.x releases, 10.1.0 and later	4	32

Table 15: Supported Compute Shapes for Firewall Management Center Virtual 300 (FMCv300)

OCI Shape	Supported Firewall Management Center Virtual 300 version	Attributes	
		oCPUs	RAM (GB)
VM.Standard2.16	7.1.0 and later	16	64 GB
Intel VM.Standard3.Flex	7.3.0 and later	16	64 GB
Intel VM.Optimized3.Flex	7.3.0 and later	16	64 GB
AMD VM.Standard.E4.Flex	7.3.0 and later	16	64 GB
AMD VM.Standard.E5.Flex	7.6.4 and later 7.6.x releases 10.1.0 and later	16	64 GB
AMD VM.Standard.E6.Flex	7.6.4 and later 7.6.x releases 10.1.0 and later	16	64 GB

Note We recommend using the Flex compute shapes.

Note Supported compute shapes availability may change by CSP.

- In OCI, 1 oCPU is equal to 2 vCPU.
- The Firewall Management Center Virtual requires 1 interface.

You create an account on OCI, launch a compute instance using the Firewall Management Center Virtual offering on the Oracle Cloud Marketplace, and choose an OCI shape.

Prerequisites

- Create an OCI account at https://www.oracle.com/cloud/.
- A Cisco Smart Account. You can create one at Cisco Software Central (https://software.cisco.com/).
  - Configure all license entitlements for the security services from the Firewall Management Center.
  - See “Licensing the System” in the Firewall Management Center Configuration Guide for more information about how to manage licenses.
- Interface requirements:
  - Management interface — One used to connect the Firewall Threat Defense device to the Firewall Management Center.
- Communications paths:
  - Public IP for administrative access to the Firewall Management Center Virtual.
- For the Firewall Management Center Virtual and System compatibility, see Cisco Secure Firewall Threat Defense Compatibility Guide.

Guidelines and Limitations

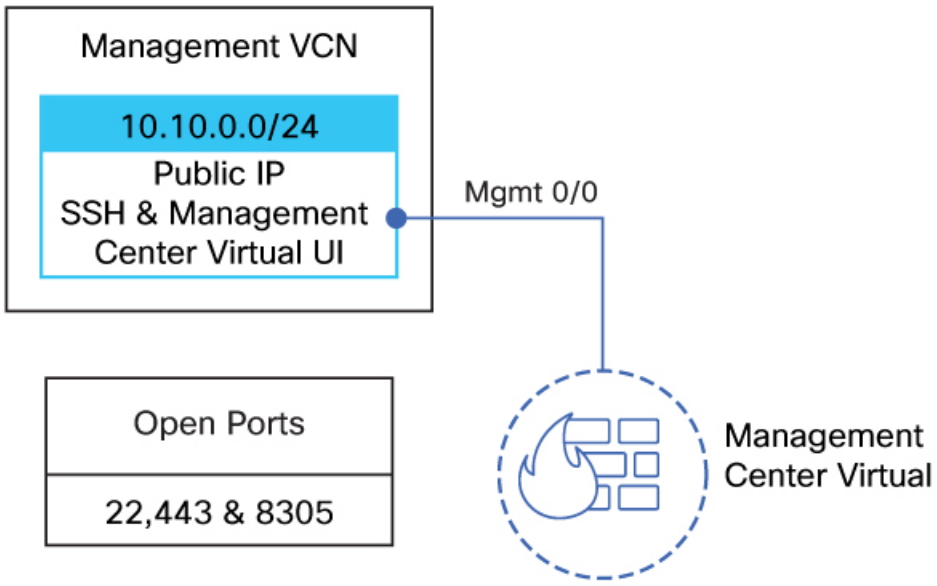
Supported Features

- Deployment in the OCI Virtual Cloud Network (VCN)
- Maximum of 8 vCPUs per instance
- Routed mode (default)
- Licensing – Only BYOL is supported
- IPv6
- **Firewall Management Center Virtual 300 (FMCv300) for OCI**—A new scaled Firewall Management Center Virtual image is available on the OCI platform that supports managing up to 300 devices and has higher disk capacity (7.1.0+).
- Firewall Management Center Virtual high availability (HA) is supported

Sample Network Topology

The following figure illustrates the typical topology for the Firewall Management Center Virtual with 1 subnet configured in OCI.

Figure 5: Topology Example for the Firewall Management Center Virtual Deployment on OCI



Deploy the Firewall Management Center Virtual

Configure the Virtual Cloud Network (VCN)

You configure the Virtual Cloud Network (VCN) for your Firewall Management Center Virtual deployment.

Before you begin

Note After you select a service from the navigation menu, the menu on the left includes the compartments list. Compartments help you organize resources to make it easier to control access to them. Your root compartment is created for you by Oracle when your tenancy is provisioned. An administrator can create more compartments in the root compartment and then add the access rules to control which users can see and take action in them. See the Oracle document "Managing Compartments" for more information.

Procedure

Step 1 Log into OCI and choose your region.

OCI is divided into multiple regions that are isolated from each other. The region is displayed in the upper right corner of your screen. Resources in one region do not appear in another region. Check periodically to make sure you are in the intended region.

Step 2 Choose **Networking** > **Virtual Cloud Networks** and click **Create VCN**.

Step 3 Enter a descriptive **Name** for your VCN, for example *FMCv-Management*.

Step 4 Enter a **CIDR block** for your VCN.

Step 5 Click **Create VCN**.

What to do next

You can continue with the following procedures to complete the Management VCN.

Create the Network Security Group

A network security group consists of a set of vNICs and a set of security rules that apply to the vNICs.

Procedure

Step 1 Choose **Networking** > **Virtual Cloud Networks** > **Virtual Cloud Network Details** > **Network Security Groups**, and click **Create Network Security Group**.

Step 2 Enter a descriptive **Name** for your Network Security Group, for example *FMCv-Mgmt-Allow-22-443-8305*.

Step 3 Click **Next**.

Step 4 Add your security rules:

a) Add a rule to allow TCP port 22 for SSH access.

b) Add a rule to allow TCP port 443 for HTTPS access.

c) Add a rule to allow TCP port 8305.

The device Firewall Management Center Virtual can be managed via the Firewall Management Center Virtual, which requires port 8305 to be opened for HTTPS connections. You need port 443 to access the Firewall Management Center itself.

Step 5 Click **Create**.

Create the Internet Gateway

An Internet gateway is required to make your management subnet publicly accessible.

Procedure

Step 1 Choose **Networking** > **Virtual Cloud Networks** > **Virtual Cloud Network Details** > **Internet Gateways**, and click **Create Internet Gateway**.

Step 2 Enter a descriptive **Name** for your Internet gateway, for example *FMCv-IG*.

Step 3 Click **Create Internet Gateway**.

Step 4 Add the route to the Internet Gateway:

a) Choose **Networking** > **Virtual Cloud Networks** > **Virtual Cloud Network Details** > **Route Tables**.

b) Click on the link for your default route table to add route rules.
c) Click **Add Route Rules**.
d) From the **Target Type** drop-down, select **Internet Gateway**.
e) Enter the Destination CIDR Block, for example 0.0.0.0/0.
f) From the **Target Internet Gateway** drop-down, select the gateway you created.
g) Click **Add Route Rules**.

Create the Subnet

Each VCN will have one subnet, at a minimum. You'll create a Management subnet for the Management VCN.

Procedure

Step 1 Choose **Networking** > **Virtual Cloud Networks** > **Virtual Cloud Network Details** > **Subnets**, and click **Create Subnet**.

Step 2 Enter a descriptive **Name** for your subnet, for example *Management*.

Step 3 Select a **Subnet Type** (leave the recommended default of **Regional**).

Step 4 Enter a **CIDR Block**, for example 10.10.0.0/24. The internal (non-public) IP address for the subnet is taken from this CIDR block.

Step 5 Select one of the route tables you created previously from the **Route Table** drop-down.

Step 6 Select the **Subnet Access** for your subnet.

For the Management subnet, this must be **Public Subnet**.

Step 7 Select the **DHCP Option**.

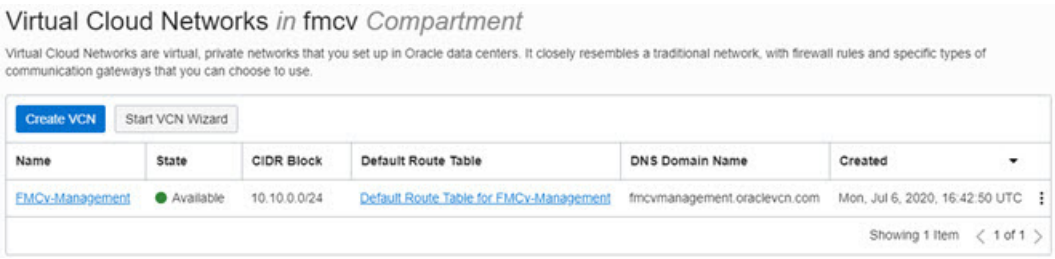
Step 8 Select a **Security List** that you created previously.

Step 9 Click **Create Subnet**.

What to do next

After you configure your Management VCN you are ready to launch the Firewall Management Center Virtual. See the following figure for an example of the Firewall Management Center Virtual VCN configuration.

Figure 6: Firewall Management Center Virtual Virtual Cloud Network



Create the Firewall Management Center Virtual Instance on OCI

You deploy the Firewall Management Center Virtual on OCI via a Compute instance using the Firewall Management Center Virtual - BYOL offering on the Oracle Cloud Marketplace. You select the most appropriate machine shape based on characteristics such as the number of CPUs, amount of memory, and network resources.

Procedure

Step 1 Log into the OCI portal.

The region is displayed in the upper right corner of your screen. Make sure you are in the intended region.

Step 2 Choose **Marketplace** > **Applications**.

Step 3 Search Marketplace for "Firewall Management Center Virtual" and choose the offering.

Step 4 Review the Terms and Conditions, and check the **I have reviewed and accept the Oracle Terms of Use and the Partner terms and conditions.**check box.

Step 5 Click **Launch Instance**.

Step 6 Enter a descriptive **Name** for your instance, for example *Cisco-FMCv*.

Step 7 Click **Change Shape** and select the shape with the number of CPUs, amount of RAM, and number of interfaces required for the Firewall Management Center Virtual, for example VM.Standard2.4 (see OCI Compute Shapes, on page 89).

Step 8 From the **Virtual Cloud Network** drop-down, choose the Management VCN.

Step 9 From the **Subnet** drop-down, choose the Management subnet if it's not autopopulated.

Step 10 Check **Use Network Security Groups to Control Traffic** and choose the security group you configured for the Management VCN.

Step 11 Click the **Assign a Public Ip Address** radio button.

Step 12 Under **Add SSH keys**, click the **Paste Public Keys** radio button and paste the SSH key.

Linux-based instances use an SSH key pair instead of a password to authenticate remote users. A key pair consists of a private key and public key. You keep the private key on your computer and provide the public key when you create an instance. See Managing Key Pairs on Linux Instances for guidelines.

Step 13 Click the **Show Advanced Options** link to expand the options.

Step 14 Under **Initialization Script**, click the **Paste Cloud-Init Script** radio button to provide the day0 configuration for the Firewall Management Center Virtual. The day0 configuration is applied during the firstboot of the Firewall Management Center Virtual.

The following example shows a sample day0 configuration you can copy and paste in the **Cloud-Init Script** field:

```
{
"AdminPassword": "myPassword@123456",
"Hostname": "cisco-fmcv"
}
```

Step 15 Click **Create**.

What to do next

Monitor the Firewall Management Center Virtual instance, which shows the state as Provisioning after you click the **Create** button. It's important to monitor the status. Look for the Firewall Management Center Virtual

instance to go from Provisioning to Running state, which indicates the Firewall Management Center Virtual boot is complete.

Access the Firewall Management Center Virtual Instance on OCI

You can connect to a running instance by using a Secure Shell (SSH) connection.

- Most UNIX-style systems include an SSH client by default.
- Windows 10 and Windows Server 2019 systems should include the OpenSSH client, which you'll need if you created your instance using the SSH keys generated by Oracle Cloud Infrastructure.
- For other Windows versions you can download PuTTY, the free SSH client from http://www.putty.org.

Prerequisites

You'll need the following information to connect to the instance:

- The public IP address of the instance. You can get the address from the Instance Details page in the Console. Open the navigation menu. Under **Core Infrastructure**, go to **Compute** and click **Instances**. Then, select your instance. Alternatively, you can use the Core Services API ListVnicAttachments and GetVnic operations.
- The username and password of your instance.
- The full path to the private key portion of the SSH key pair that you used when you launched the instance.

  For more information about key pairs, see Managing Key Pairs on Linux Instances.

Note If you choose not to add a Day0 configuration, you can log in to the Firewall Management Center Virtual instance using the default credentials (admin/Admin123).

You are prompted to set the password on the first login attempt.

Connect to the Firewall Management Center Virtual Instance Using PuTTY

To connect to the Firewall Management Center Virtual instance from a Windows system using PuTTY:

Procedure

Step 1 Open PuTTY.

Step 2 In the **Category** pane, select **Session** and enter the following:

- **Host Name (or IP address):**

```
<username>@<public-ip-address>
```

Where:

<username> is the username for the Firewall Management Center Virtual instance.

<public-ip-address> is your instance public IP address that you retrieved from the Console.

- **Port:** 22
- **Connection type:** SSH

Step 3 In the **Category** pane, expand **Window**, and then select **Translation**.

Step 4 In the **Remote character set** drop-down list, select **UTF-8**.

The default locale setting on Linux-based instances is UTF-8, and this configures PuTTY to use the same locale.

Step 5 In the **Category** pane, expand **Connection**, expand **SSH**, and then click **Auth**.

Step 6 Click **Browse**, and then select your private key.

Step 7 Click **Open** to start the session.

If this is your first time connecting to the instance, you might see a message that the server's host key is not cached in the registry. Click **Yes** to continue the connection.

Connect to the Firewall Management Center Virtual Instance Using SSH

To connect to the Firewall Management Center Virtual instance from a Unix-style system, log in to the instance using SSH.

Procedure

Step 1 Use the following command to set the file permissions so that only you can read the file:

```
$ chmod 400 <private_key>
```

Where:

<private_key> is the full path and name of the file that contains the private key associated with the instance you want to access.

Step 2 Use the following SSH command to access the instance:

```
$ ssh -i <private_key> <username>@<public-ip-address>
```

<private_key> is the full path and name of the file that contains the private key associated with the instance you want to access.

<username> is the username for the Firewall Management Center Virtual instance.

<public-ip-address> is your instance IP address that you retrieved from the console.

Connect to the Firewall Management Center Virtual Instance Using OpenSSH

To connect to the Firewall Management Center Virtual instance from a Windows system, log in to the instance using OpenSSH.

Procedure

Step 1 If this is the first time you are using this key pair, you must set the file permissions so that only you can read the file.

Do the following:

a) In Windows Explorer, navigate to the private key file, right-click the file, and then click **Properties**.
b) On the **Security** tab, click **Advanced**.
c) Ensure that the **Owner** is your user account.
d) Click **Disable Inheritance**, and then select **Convert inherited permissions into explicit permissions on this object**.
e) Select each permission entry that is not your user account and click **Remove**.
f) Ensure that the access permission for your user account is **Full control**.
g) Save your changes.

Step 2 To connect to the instance, open Windows PowerShell and run the following command:

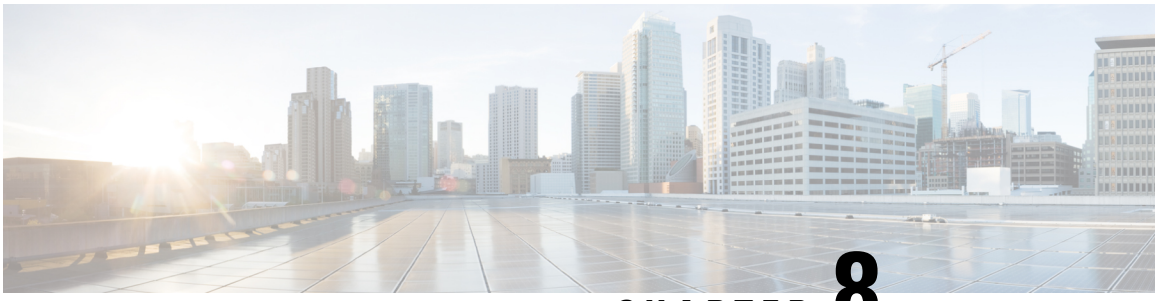
```
$ ssh -i <private_key> <username>@<public-ip-address>
```

Where:

`<private_key>` is the full path and name of the file that contains the private key associated with the instance you want to access.

`<username>` is the username for the Firewall Management Center Virtual instance.

`<public-ip-address>` is your instance IP address that you retrieved from the Console.



CHAPTER 8

Deploy the Firewall Management Center Virtual on OpenStack

You can deploy the Firewall Management Center Virtual on OpenStack.

- Overview, on page 99
- Prerequisites, on page 99
- Guidelines and Limitations, on page 100
- System Requirements, on page 101
- Sample Network Topology, on page 102
- Deploy the Firewall Management Center Virtual, on page 103

Overview

This guide describes how to deploy the Firewall Management Center Virtual in an OpenStack environment. OpenStack is a free open standard cloud computing platform, mostly deployed as infrastructure-as-a-service (IaaS) in both public and private clouds where virtual servers and other resources are made available to users.

The Firewall Management Center Virtual runs the same software as physical Firewall Management Center to deliver proven security functionality in a virtual form factor. The Firewall Management Center Virtual can be deployed on OpenStack. It can then be configured to manage virtual and physical devices.

This deployment uses a KVM hypervisor to manage virtual resources. KVM is a full virtualization solution for Linux on x86 hardware containing virtualization extensions (such as Intel VT). It consists of a loadable kernel module, kvm.ko, that provides the core virtualization infrastructure and a processor specific module, such as kvm-intel.ko. You can run multiple virtual machines running unmodified OS images using KVM. Each virtual machine has private virtualized hardware: a network card, disk, graphics adapter, and so forth.

Because the devices are already supported on the KVM hypervisor, no additional kernel packages or drivers are needed to enable OpenStack support.

Prerequisites

- Download the Firewall Management Center Virtual qcow2 file from software.cisco.com and put it on your Linux host:

  https://software.cisco.com/download/navigator.html

- A software.cisco.com and Cisco service contract are required.
- The Firewall Management Center Virtual supports deployment on RHEL OpenStack environment and Cisco VIM managed OpenStack environment.
- Licensing:
  - You configure license entitlements for the security services from the Firewall Management Center.
  - See “Licensing the System” in the *Secure Firewall Management Center Configuration Guide* for more information about how to manage licenses.
- Memory and resource requirements:
  - Processors
    - Requires 4 vCPUs or 8 vCPUs
  - Memory
    - Minimum required 28 GB / Recommended (default) 32 GB RAM
  - Host storage per Virtual Machine
    - The Firewall Management Center Virtual requires 250 GB



Note You can modify the vCPU and memory values as per your requirement.

- Interface requirements:
  - Management interface — One used to connect the device to the Firewall Management Center.
- Communications paths:
  - Floating IPs for access into the Firewall Management Center Virtual.
- Minimum supported Firewall Management Center Virtual version:
  - Version 7.0.
- For OpenStack requirements, see System Requirements, on page 101.
- For Firewall Management Center Virtual and System compatibility, see Cisco Secure Firewall Threat Defense Compatibility Guide.

Guidelines and Limitations

Supported Features

The Firewall Management Center Virtual on OpenStack supports the following features:

- Deployment the Firewall Management Center Virtual on the KVM hypervisor running on a compute node in your OpenStack environment.
- OpenStack CLI
- Heat template-based deployment
- Licensing — Only BYOL is supported
- Drivers - VIRTIO
- IPv6 is supported

Unsupported Features

The Firewall Management Center Virtual on OpenStack does not support the following:

- Autoscale
- Cluster

Note Firewall Device Manager is not supported on OpenStack.

System Requirements

The OpenStack environment must conform to the following supported hardware and software requirements.

Table 16: Hardware and Software Requirements for RHEL

Category	Supported Versions	Notes
Server	UCS C220-M5/UCS C240-M4	2 UCS servers are recommended, one each for os-controller and os-compute nodes.
Driver	VIRTIO	These are the supported drivers.
Operating System	Red Hat OpenStack Platform 17.1.13 with the OpenStack Wallaby release on Red Hat Enterprise Linux release 9.8 (Plow)	
OpenStack Version	Red Hat OpenStack Platform release 17.1.13 (Wallaby)	

Table 17: Hardware and Software Requirements for Cisco VIM Managed OpenStack

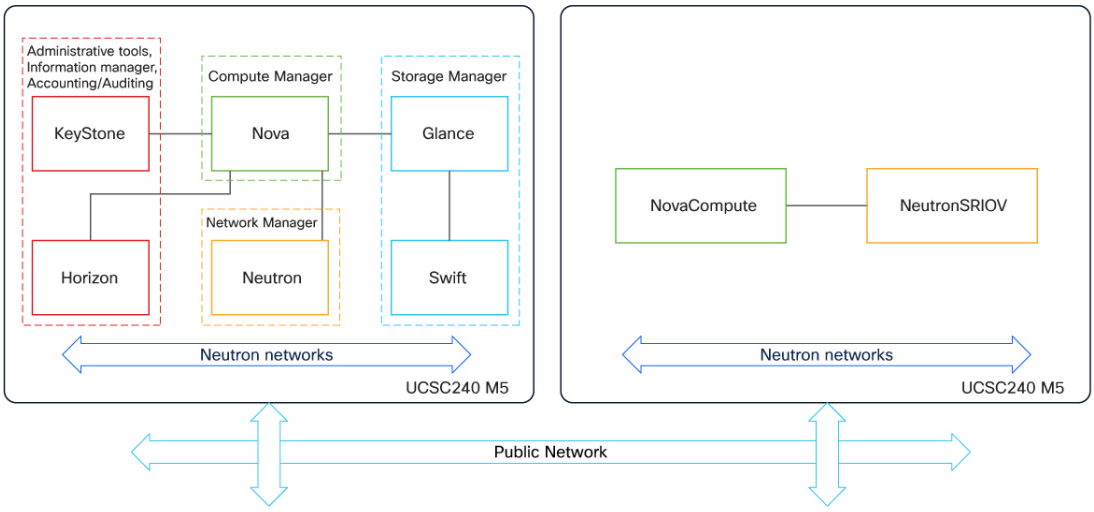
Category	Supported Versions	Notes
Server Hardware	UCS C220-M5/UCS C240-M4	5 UCS servers are recommended, three each for os-controller and Two or more for os-compute nodes.

Category	Supported Versions	Notes
Drivers	VIRTIO	These are the supported drivers.
HVIM Version	HVIM 6.0.0 Supported on: • Red Hat Enterprise Linux (RHEL) 9.4 • OSP 18 (OpenStack 2023.1 Antelope)	See HVIM 6.0.0 - Red Hat Enterprise Linux (RHEL) 9.4 and OSP 18 (OpenStack 2023.1 Antelope) for more information.

OpenStack Platform Topology

The following figure shows the recommended topology to support deployments in OpenStack using two UCS servers.

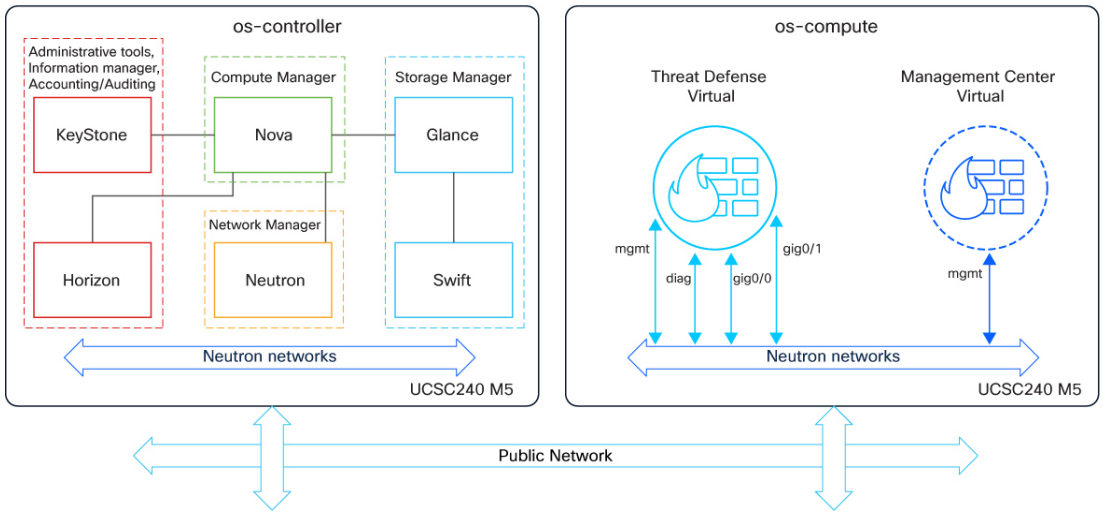
Figure 7: OpenStack Platform Topology



Sample Network Topology

The following figure shows a network topology example for the Firewall Management Center Virtual in OpenStack.

Figure 8: Topology Example with the Firewall Management Center Virtual on OpenStack



Deploy the Firewall Management Center Virtual

Cisco provides sample heat templates for deploying the Firewall Management Center Virtual. Steps for creating the OpenStack infrastructure resources are combined in a heat template (`deploy_os_infra.yaml`) file to create networks, subnets, and router interfaces. At a high-level, the Firewall Management Center Virtual deployment steps are categorized into the following sections.

- Upload the Firewall Management Center Virtual qcow2 image to the OpenStack Glance service.
- Create the network infrastructure.
  - Network
  - Subnet
  - Router interface
- Create the Firewall Management Center Virtual instance.
  - Flavor
  - Security Groups
  - Floating IP
  - Instance

You can deploy the Firewall Management Center Virtual on OpenStack using the following steps.

Upload the Firewall Management Center Virtual Image to OpenStack

Copy the Firewall Management Center Virtual qcow2 image to the OpenStack controller node, and then upload the image to the OpenStack Glance service.

Before you begin

- Download the Firewall Management Center Virtual qcow2 file from Cisco.com and put it on your Linux host:

  https://software.cisco.com/download/navigator.html

Procedure

Step 1 Copy the qcow2 image file to the OpenStack controller node.

Step 2 Upload the Firewall Management Center Virtual image to the OpenStack Glance service.

```
root@ucs-os-controller:$ openstack image create <fmcv_image> --public --disk-
format qcow2 --container-format bare --file ./<fmcv_qcow2_file>
```

Step 3 (Valid for Firewall Management Center Virtual 10.0.0 and later versions) If the OpenStack environment is running Red Hat Enterprise Linux (RHEL) 9 or later, set the image property for the uploaded image.

```
openstack image set <image_id> --property hw_machine_type=pc
```

Example:

```
openstack image set 06dd7975-0b6e-45b8-810a-4ff98546a39d --property hw_machine_type=pc
```

Step 4 Verify if the Firewall Management Center Virtual image upload is successful.

root@ucs-os-controller:$ openstack image list

Example:

```
root@ucs-os-controller:$ openstack image list
+--------------------------------------+-------------------+---------+
| ID                                   | Name              | Status |+
| b957b5f9-ed1b-4975-b226-4cddf5887991 | fmcv-7-0-image    | active |+
```

The uploaded image and its status is displayed.

What to do next

Create the network infrastructure using the `deploy_os_infra.yaml` template.

Create the Network Infrastructure for the OpenStack and the Firewall Management Center Virtual

Deploy the OpenStack infrastructure heat template to create the network infrastructure.

Before you begin

Heat template files are required to create the network infrastructure and the required components for the Firewall Management Center Virtual, such as flavor, networks, subnets, router interfaces, and security group rules:

- `env.yaml` — Defines the resources created to support the Firewall Management Center Virtual on the compute node, such as the image name, interfaces, and IP addresses.

- `deploy_os_infra.yaml` — Defines the environment for the Firewall Management Center Virtual, such as the network and subnets.

Templates for your Firewall Management Center Virtual version are available from the GitHub repository at FMCv OpenStack heat template.

Important Note that Cisco-provided templates are provided as open source examples, and are not covered within the regular Cisco TAC support scope. Check GitHub regularly for updates and ReadMe instructions.

Procedure

Step 1 Deploy the infrastructure heat template file.

root@ucs-os-controller:$ openstack stack create <stack-name> -e <environment files name> -t <deployment file name>

Example:

```
root@ucs-os-controller:$ openstack stack create infra-stack -e env.yaml -t deploy_os_infra.yaml
```

Step 2 Verify if the infrastructure stack is created successfully.

root@ucs-os-controller:$ openstackstack list

Example:

```
root@ucs-os-controller:$ openstack stack list
+--------------------------------------+------------+----------------------------------+-----------------+
| ID                                   | Stack Name  | Project                          | Stack Status
    |
+--------------------------------------+------------+----------------------------------+-----------------+
| b30d5875-ce3a-4258-a841-bf2d09275929 | infra-stack | 13206e49b48740fdafca83796c6f4ad5 |
CREATE_COMPLETE |
+--------------------------------------+------------+----------------------------------+-----------------+
```

What to do next

Create the Firewall Management Center Virtual instance on OpenStack.

Create the Firewall Management Center Virtual Instance on OpenStack

Use the sample heat template to deploy the Firewall Management Center Virtual on OpenStack.

Before you begin

A heat template is required to deploy the Firewall Management Center Virtual on OpenStack:

- `deploy_fmcv.yaml`

Templates for your Firewall Management Center Virtual version are available from the GitHub repository at FMCv OpenStack heat template.



Important Note that Cisco-provided templates are provided as open source examples, and are not covered within the regular Cisco TAC support scope. Check GitHub regularly for updates and ReadMe instructions.

Procedure

Step 1 Deploy the Firewall Management Center Virtual heat template file (`deploy_fmcv.yaml`) to create the Firewall Management Center Virtual instance.

root@ucs-os-controller:$ openstack stack create fmcv-stack -e env.yaml-t deploy_fmcv.yaml

Example:

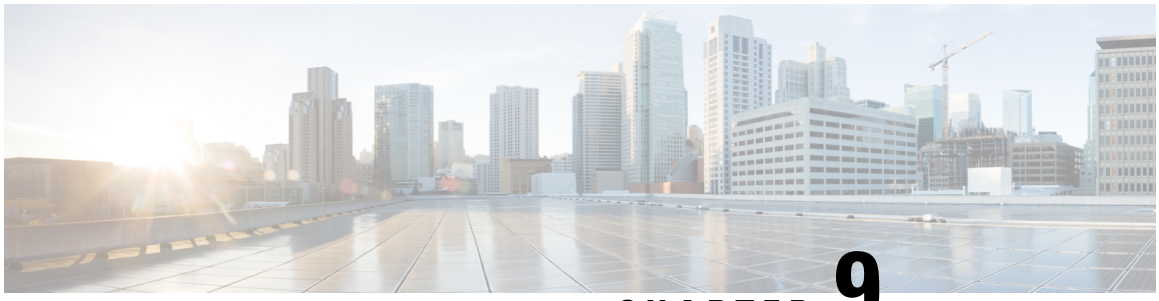
```
+---------------------+------------------------------+
| Field               | Value                        |
+---------------------+------------------------------+
| id                  | 96c8c126-107b-4733-8f6c-eb15a637219f |
| stack_name          | fmcv-stack                   |
| description         | FMCv template                |
| updated_time        | None                         |
| stack_status        | CREATE_IN_PROGRESS           |
| stack_status_reason | Stack CREATE started         |
+---------------------+------------------------------+
```

Step 2 Verify that your Firewall Management Center Virtual stack is created successfully.

root@ucs-os-controller:$ openstack stack list

Example:

```
+--------------------------------------+-------------+----------------------------------+--------+
| ID                                   | Stack Name  | Project                          | Stack Status
    |
+--------------------------------------+-------------+----------------------------------+-----------------+
| 14624af1-e5fa-4096-bd86-c453bc2928ae | fmcv-stack  | 13206e49b48740fdafca83796c6f4ad5 |
CREATE_COMPLETE |
| 198336cb-1186-45ab-858f-15ccd3b909c8 | infra-stack | 13206e49b48740fdafca83796c6f4ad5 |
CREATE_COMPLETE |
+--------------------------------------+-------------+----------------------------------+-----------------+
```



CHAPTER 9

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 107
- Deploy the Firewall Management Center Virtual, on page 110
- Power On and Initialize the Virtual Appliance, on page 111

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 18: 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 19: 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, on page 22

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.

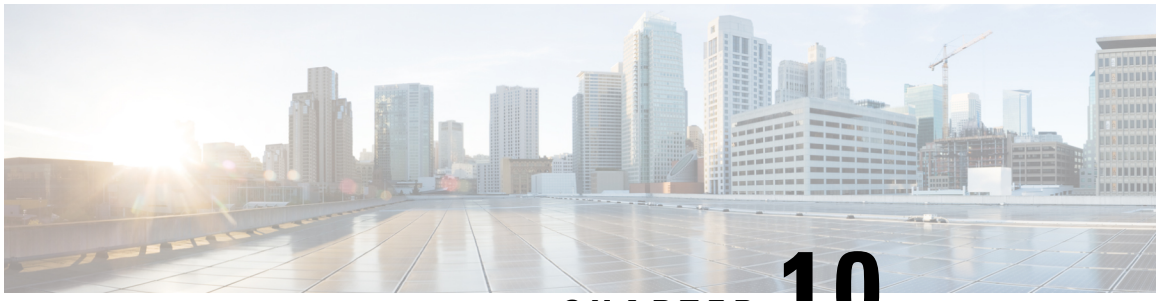
In the vSphere Client, right-click the name of your virtual appliance from the inventory list, then select **Power** > **Power On** from the context menu.

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, on page 137.
- 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.



CHAPTER 10

Deploy the Firewall Management Center Virtual on Nutanix

Nutanix AHV is a native bare metal Type-1 hypervisor, Hyper-converged Infrastructure HCI with cloud enabled features and functionality.

This chapter describes how the Firewall Management Center Virtual functions in the Nutanix environment with AHV hypervisor, including feature support, system requirements, guidelines, and limitations.

You can deploy the Firewall Management Center Virtual on Nutanix AHV.

- Overview, on page 113
- Deploy the Firewall Management Center Virtual on Nutanix, on page 116

Overview

Nutanix AHV is a native bare metal Type-1 hypervisor, Hyper-converged Infrastructure HCI with cloud enabled features and functionality.

This chapter describes how the Firewall Management Center Virtual functions in the Nutanix environment with AHV hypervisor, including feature support, system requirements, guidelines, and limitations.

You can deploy the Firewall Management Center Virtual on Nutanix AHV.

System Requirements

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.

Supported Management Center Virtual models

- FMCv2 and FMCv10
- FMCv25 (Secure Firewall version 10.1 and later)

Memory and Resource Requirements

- You can run multiple virtual machines running unmodified OS images using Nutanix AHV. Each virtual machine has private virtualized hardware: a network card, disk, graphics adapter, and so forth. See the Cisco Secure Firewall Threat Defense Compatibility Guide for hypervisor compatibility.
- Check for 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 lists the recommended and default settings for the Firewall Management Center Virtual appliance on Nutanix AHV:
- Processors
  - Requires 4 vCPUs
- Memory
  - Minimum required 28 GB / Recommended (default) 32 GB RAM



Important The Firewall Management Center Virtual platform fails if you allocate less than 28 GB RAM to the virtual appliance.

- Networking
  - Supports virtio drivers
  - Supports one management interface
- Host storage per Virtual Machine
  - The Firewall Management Center Virtual requires 250 GB
  - Supports virtio and scsi block devices
- Console
  - Supports terminal server via telnet

Prerequisites

See the Cisco Secure Firewall Threat Defense Compatibility Guide for the most current information about hypervisor support for the Firewall Threat Defense Virtual.

Download the Firewall Management Center qcow2 file from Cisco.com and put it on your Nutanix Prism Web Console:

https://software.cisco.com/download/navigator.html

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

Firewall Management Center Virtual Licenses

- Configure all license entitlements for the security services from the Firewall Management Center.
- See *Licensing the System* in the Secure Firewall Management Center Configuration Guide for more information about how to manage licenses.

Nutanix Components and Versions

Component	Version
Nutanix Acropolis Operating System (AOS)	5.15.5 LTS and later without VPC support. 6.8 and later with VPC support.
Nutanix Cluster Check (NCC)	4.0.0.1
Nutanix AHV	20201105.12 and later
Nutanix Prism Web Console	-

Guidelines and Limitations

Supported Features

Deployment Modes:

- Standalone
- High availability - supported on FMCv25 from Secure Firewall version 10.1

Unsupported Features

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.

- Nested hypervisors (Nutanix AHV running on top of ESXi) are not supported. Only Nutanix standalone cluster deployments are supported.
- Nutanix AHV does not support SR-IOV and DPDK-OVS

Note Firewall Device Manager is not supported on Nutanix.

Related Documentation

- Nutanix Release Notes
- Nutanix Field Installation Guide
- Hardware Support on Nutanix

Deploy the Firewall Management Center Virtual on Nutanix

Step	Task	More Information
1	Review the prerequisites.	Prerequisites, on page 114
2	Upload the Firewall Management Center Virtual qcow2 file to the Nutanix environment.	Upload the Firewall Management Center Virtual QCOW2 File to Nutanix, on page 116
3	(Optional) Prepare a Day 0 configuration file that contains the initial configuration data that gets applied at the time a virtual machine is deployed.	Prepare the Day 0 Configuration File, on page 117
4	Deploy the Firewall Management Center Virtual to the Nutanix environment.	Deploy the Management Center Virtual to Nutanix
5	(Optional) If you did not use a Day 0 configuration file to set up the Firewall Management Center Virtual, complete the setup by logging in to the CLI.	Complete the Firewall Management Center Virtual Setup, on page 120

Upload the Firewall Management Center Virtual QCOW2 File to Nutanix

To deploy the Firewall Management Center Virtual to the Nutanix environment, you must create an image from the Firewall Management Center Virtual qcow2 disk file in the Prism Web Console.

Before you begin

Download the Firewall Management Center Virtual qcow2 disk file from Cisco.com: https://software.cisco.com/download/navigator.html

Procedure

Step 1 Log in to the Nutanix Prism Web Console.

Step 2 Click the gear icon to open the **Settings** page.

Step 3 Click **Image Configuration** from the left pane.

Step 4 Click **Upload Image**.

Step 5 Create the image.

a. Enter a name for the image.

b. From the **Image Type** drop-down list, choose **DISK**.

c. From the **Storage Container** drop-down list, choose the desired container.

d. Specify the location of the Firewall Management Center Virtual qcow2 disk file.

   You can either specify a URL (to import the file from a web server) or upload the file from your workstation.

e. Click **Save**.

Step 6 Wait until the new image appears in the **Image Configuration** page.

Prepare the Day 0 Configuration File

You can prepare a Day 0 configuration file before you deploy the Firewall Management Center Virtual. This file is a text file that contains the initial configuration data that gets applied at the time a virtual machine is deployed.

Keep in mind that:

- If you deploy with a Day 0 configuration file, the process allows you to perform the entire initial setup for the Firewall Management Center Virtual appliance.
- If you deploy without a Day 0 configuration file, you must configure System-required settings after launch; see Complete the Firewall Management Center Virtual Setup, on page 120 for more information.

You can specify:

- The End User License Agreement (EULA) acceptance.
- A hostname for the system.
- A new administrator password for the admin account.
- Network settings that allow the appliance to communicate on your management network.

Procedure

Step 1 Create a new text file using a text editor of your choice.

Step 2 Enter the configuration details in the text file as shown in the following sample. Note that the text is in JSON format. You can validate the text using a validator tool before copying the text.

Example:

```
#FMC
{
    "EULA": "accept",
    "Hostname": "FMC-Production",
    "AdminPassword": "Admin123",
    "DNS1": "10.1.1.5",
    "DNS2": "192.168.1.67",
    "IPv4Mode": "manual",
```

```
    "IPv4Addr": "10.12.129.45",
    "IPv4Mask": "255.255.0.0",
    "IPv4Gw": "10.12.0.1",
    "IPv6Mode": "disabled",
    "IPv6Addr": "",
    "IPv6Mask": "",
    "IPv6Gw": "",
}
```

Step 3 Save the file as "**day0-config.txt**."

Step 4 Repeat Step 1–3 to create unique default configuration files for each Firewall Management Center Virtual that you want to deploy.

Deploy the Firewall Management Center Virtual to Nutanix

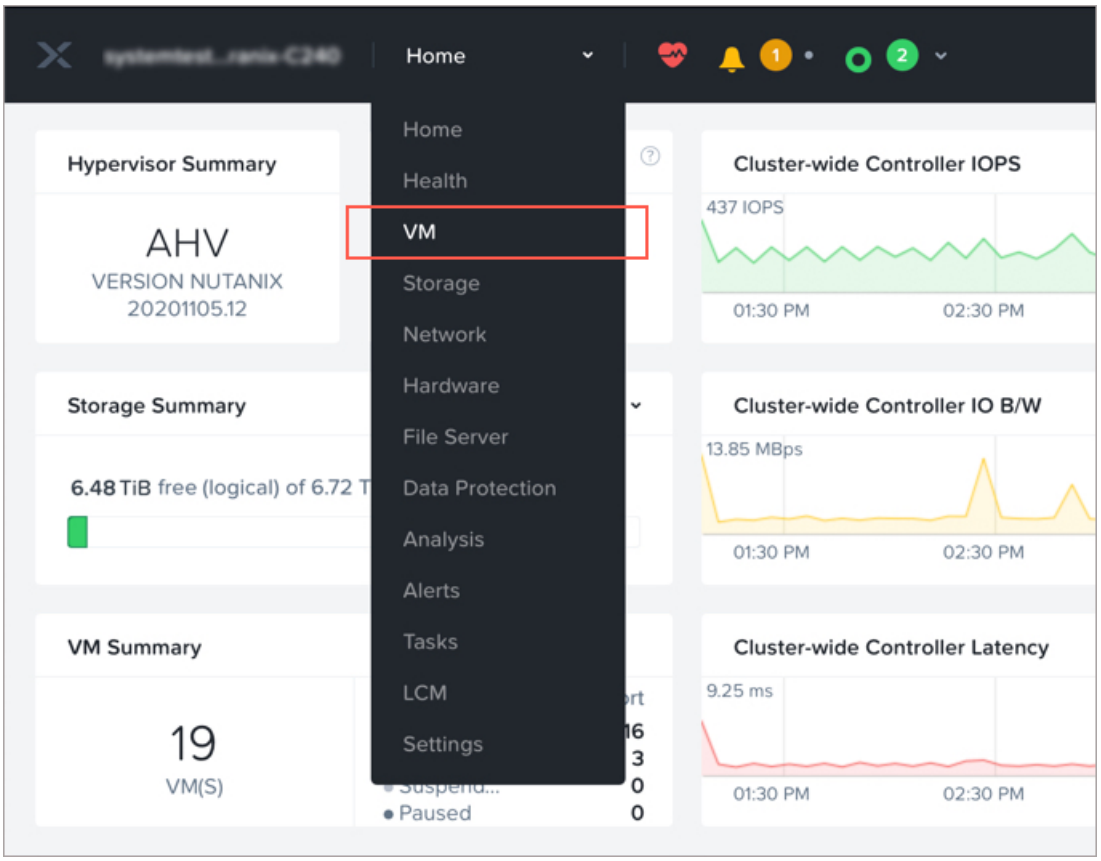
Before you begin

Ensure that the image of the Firewall Management Center Virtual that you plan to deploy is appearing on the **Image Configuration** page.

Procedure

Step 1 Log in to the Nutanix Prism Web Console.

Step 2 From the main menu bar, click the view drop-down list, and choose **VM**.



Step 3 On the VM Dashboard, click **Create VM**.

Step 4 Do the following:

a. Enter a name for the Firewall Management Center Virtual instance.

b. Optionally enter a description for the Firewall Management Center Virtual instance.

c. Select the timezone that you want the Firewall Management Center Virtual instance to use.

Step 5 Enter the compute details.

a. Enter the number of virtual CPUs to allocate to the Firewall Management Center Virtual instance.

b. Enter the number of cores that must be assigned to each virtual CPU.

c. Enter the amount of memory (in GB) to allocate to the Firewall Management Center Virtual instance.

Step 6 Attach a disk to the Firewall Management Center Virtual instance.

a. Under **Disks**, Click **Add New Disk**.

b. From the **Type** drop-down list, choose **DISK**.

c. From the **Operation** drop-down list, choose **Clone from Image Service**.

d. From the **Bus Type** drop-down list, choose **SCSI**, **PCI**, or **SATA**.

e. From the **Image** drop-down list, choose the image that you want to use.

f. Click **Add**.

Step 7 Under **Network Adapters (NIC)**, click **Add New NIC**, select a network, and click **Add**.

Step 8 Configure affinity policy for the Firewall Management Center Virtual.

Under **VM Host Affinity** , click **Set Affinity**, select the hosts, and click **Save**.

Select more than one host to ensure that the Firewall Management Center Virtual can be run even if there is a node failure.

Step 9 If you have prepared a Day 0 configuration file, do the following:

a. Select **Custom Script**.

b. Click **Upload A File**, and choose the Day 0 configuration file (**day0-config.txt**).

Note All the other custom script options are not supported in this release.

Step 10 Click **Save** to deploy the Firewall Management Center Virtual. The Firewall Management Center Virtual instance appears in the VM table view.

Step 11 Create and attach a virtual serial port to the Management Center Virtual. To do this, log in to a Nutanix Controller VM (CVM) with SSH and run the Acropolis CLI (aCLI) commands given below. For more information on aCLI, see the aCLI Command Reference.

Commands for Nutanix AHV version 6.8 and below:

vm.serial_port_create <*management-center-virtual-VM-name*> **type=kServer index=0**

vm.update <*management-center-virtual-VM-name*> **disable_branding=true**

vm.update <*management-center-virtual-VM-name*> **extra_flags="enable_hyperv_clock=False"**

Commands for Nutanix AHV version 6.8.1 and above:

vm.serial_port_create <*management-center-virtual-VM-name*> **type=kServer index=0**

vm.update <*management-center-virtual-VM-name*> **disable_branding=true**

vm.update <*management-center-virtual-VM-name*> **disable_hyperv=True**

Step 12 Go to the VM table view, select the newly created the Firewall Management Center Virtual instance, and click **Power On**.

Step 13 After the Firewall Management Center Virtual is powered on, verify the status. Go to **Home > VM >** Firewall Management Center Virtual that you deployed and log in.

Complete the Firewall Management Center Virtual Setup

For all Firewall Management Centers, you must complete a setup process that allows the appliance to communicate on your management network. If you deploy without a Day 0 configuration file, setting up the Firewall Management Center Virtual is a two-step process:

Procedure

Step 1 After you initialize the Firewall Management Center Virtual, run a script at the appliance console that helps you configure the appliance to communicate on your management network.

Step 2 Then, complete the setup process using a computer on your management network to browse to the web interface of the Firewall Management Center Virtual.

Step 3 Complete the initial setup on Firewall Management Center Virtual using the CLI. See Configure Network Settings Using a Script, on page 121.

Step 4 Complete the setup process using a computer on your management network to browse to the web interface of the Firewall Management Center Virtual. See Perform Initial Setup Using the Web Interface, on page 122.

Configure Network Settings Using a Script

The following procedure describes how you complete the initial setup on the Firewall Management Center Virtual using the CLI.

Procedure

Step 1 At the console, log into the Firewall Management Center Virtual appliance. Use **admin** as the username and **Admin123** as the password. If you are using the Nutanix console, the default password is **Admin123**.

If prompted, reset the password.

Step 2 At the admin prompt, run the following script:

Example:

```
sudo /usr/local/sf/bin/configure-network
```

On first connection to the Firewall Management Center Virtual you are prompted for post-boot configuration.

Step 3 Follow the script's prompts.

Configure (or disable) IPv4 management settings first, then IPv6. If you manually specify network settings, you must enter IPv4 or IPv6 address.

Step 4 Confirm that your settings are correct.

Step 5 Log out of the appliance.

What to do next

- Complete the setup process using a computer on your management network to browse to the web interface of the Firewall Management Center Virtual.

Perform Initial Setup Using the Web Interface

The following procedure describes how you complete the initial setup on the Firewall Management Center Virtual using the web interface.

Procedure

Step 1 Direct your browser to default IP address of the Firewall Management Center Virtual's management interface:

Example:

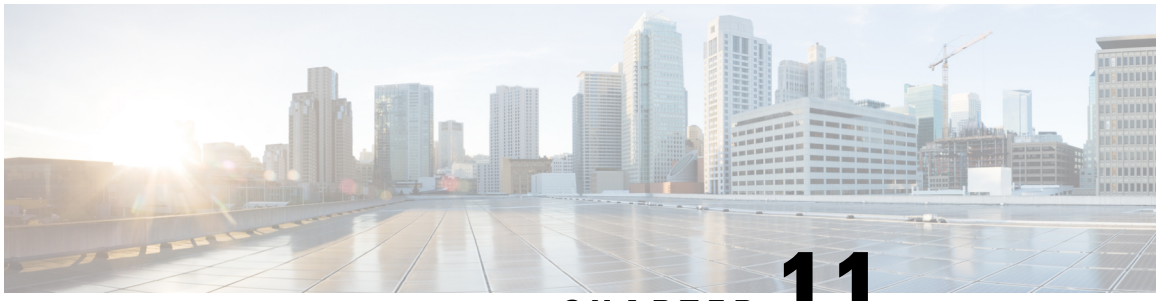
```
https://192.168.45.45
```

Step 2 Log into the Firewall Management Center Virtual appliance. Use **admin** as the username and **Admin123** as the password. If prompted, reset the password.

The setup page appears. You must change the administrator password, specify network settings if you haven't already, and accept the EULA.

Step 3 When you are finished, click **Apply**. The Firewall Management Center Virtual is configured according to your selections. After an intermediate page appears, you are logged into the web interface as the admin user, which has the Administrator role.

The Firewall Management Center Virtual is configured according to your selections. After an intermediate page appears, you are logged into the web interface as the admin user, which has the Administrator role.



CHAPTER 11

Deploy the Firewall Management Center Virtual on Alibaba Cloud

- Overview, on page 123
- Guidelines and Limitations, on page 124
- Prerequisites, on page 125
- Deploy the Firewall Management Center Virtual, on page 125

Overview

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. If you allocate less than 28 GB RAM to the virtual appliance, then the Firewall Management Center Virtual upgrades to Version 6.6.0+ fails.

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

Note The Management Center Virtual on Alibaba Cloud is supported on Secure Firewall version 7.2 and later releases.

Alibaba Cloud Supported Instance Types

Management Center Virtual on Alibaba Cloud can use the instance types mentioned in the following table:

Configuration	No of vCPUs	Memory (GB)	Maximum Interfaces Supported	Supported version
ecs.r6.xlarge	4	32	4	7.2 or later
ecs.r8i.xlarge	4	32	4	7.2 or later
ecs.g8i.2xlarge	8	32	4	7.2 or later

Configuration	No of vCPUs	Memory (GB)	Maximum Interfaces Supported	Supported version
ecs.r9i.xlarge	4	32	4	7.2 or later
ecs.g9i.2xlarge	8	32	4	7.2 or later
ecs.r8i.2xlarge	8	64	4	10.1.0 or above
ecs.g9i.2xlarge	8	32	4	10.1.0 or above
ecs.r9i.2xlarge	8	64	4	10.1.0 or above



Note Management center virtual needs a minimum of one interface (ENI) to support the instance.

Network Requirement

- Create one VPC with a minimum of one Vswitch (Subnet) for basic management center virtual support.
- You must create a Vswitch, if the Vswitch is not available in the same zone in which instance is being deployed.

Related Documentation

For more information on instance types and their configurations, see Alibaba Cloud

Guidelines and Limitations

Supported Features

- QCOW2 Image package
- Basic Product Bringup
- Day-0 Configuration
- SSH using Public Key or Password.
- Alibaba Cloud UI Stop/Restart
- Instance Type Supported: ecs.r6.xlarge.
- BYOL License Support

Unsupported Features

- FDM
- High Availability

- Auto scaling
- IPv6
- SR-IOV

Limitations

- Transparent, inline, and passive modes are not supported in Alibaba Cloud.
- East-West Traffic is not supported in Alibaba Cloud.
- Jumbo Frames is not supported as its availability is limited to a few instance types from Alibaba Cloud. For more information, see Alibaba Cloud

Prerequisites

- An Alibaba Cloud account. You can create one at https://www.alibaba.com/.
- An SSH client (for example, PuTTY on Windows or Terminal on Macintosh) is required to access the Management Center Virtual console.
- Download the Management Center Virtual QCOW2 file from Cisco.com.
- https://software.cisco.com/download/navigator.html

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

- A Cisco Smart Account. You can create one at Cisco Software Central. https://software.cisco.com/
- Configure all license entitlements for the security services from the Firewall Management Center.
- See "Licenses" in the Secure Firewall Management Center Administration Guide for more information on how to manage licenses.

Deploy the Firewall Management Center Virtual

You must ensure that the image of the management center virtual that you plan to deploy appears on the **Image Configuration**.

Procedure

Step 1 Log into https://www.alibabacloud.com/ and choose your region.

Note Alibaba Cloud is divided into multiple regions that are isolated from each other. The region is displayed in the upper right corner of your window. Resources in one region do not appear in another region. Check periodically to make sure you are in the intended region.

Step 2 **Create Custom Virtualized Image.**

Alibaba Cloud supports a QCOW2 image only.

a) Go to Object Storage Service (OSS), then create a bucket that contains the QCOW2 image and do the following:

Bucket names must be globally unique within your Alibaba Cloud project.

1. Upload QCOW2 image from local directory to the Alibaba Cloud bucket.
2. From the left navigation pane, click **Buckets** > **management center virtualbucket** > **Upload**
3. Choose **Private** as ACL and copy the OSS Object address mentioned in the object details after the upload is completed successfully.
4. Paste the OSS object address of custom image from the bucket.
5. Choose **Linux** as OS and **Others Linux** as variant type.
6. Choose **x86_64** as System Architecture.
7. Choose Image format as **QCOW2.**
8. Choose license type as BYOL.

b) Create an instance from the para-virtualized image from the previous step.

1. From the left navigation pane, click **Images** > **Custom Image** > **Actions** > **Create Instance**

Step 3 **Create Instance from Custom Virtualized Image.**

a) Go to the **Elastic Compute Service** > **Create Instance** and select the following:

1. **Billing Method**: Pay-As-You-Go
2. **Region**: As per requirement.
3. **Instance Type**: ecs.r6.xlarge
4. **Quantity**: As required
5. **Image**: Custom image you created in the previous section.
6. **System Disk**: 250GB (or Default) as the minimum value.

b) To proceed further, do the following:

1. **VPC**: VPC in which management center virtual will be deployed.
2. **Vswitch**: Subnet of the Primary Interface.
3. **Assign Public IPv4 Address:** It is required to connect using SSH (If not selected, then the management center virtual can only be accessed via Console connection of Alibaba Cloud from the UI).

4. **Security Group**: Choose the appropriate Security Group.
5. **Interfaces**: Primary interface belongs to the subnet chosen in step 2. Management center virtual requires one interface only.

c) Move to the next section and do the following.

1. **Key-Pair**: For key-based login, generate a key-pair if not done already. You can also access the instance with a password.



Note You can select an existing key pair or create a new key pair. The key pair consists of a public key that Alibaba Cloud stores and a private key file that the user stores. Together, they allow you to connect to your instance securely. Be sure to save the key pair to a known location, as it may required to connect to the instance.

2. **Instance-name**: Name of instance as suitable.
3. **Day-0 (User Data)**: Provide the Day-0 configuration as per the requirement (Do not choose **64-base** encoded).

Sample Day-0 Configuration to manage management center virtual using the Management Center:

```
#FMC
{
"AdminPassword": "<enter_your_password>",
"Hostname": "<Hostname-vFMC>"
}
```



Note In case the user does not provide any password in the day-0 configuration, the default password will be the instance ID of the FMCv as seen on Alibaba Cloud console or CLI.

d) Accept the Terms of Service and Create the Instance.

Step 4 Click **Review and Launch**.

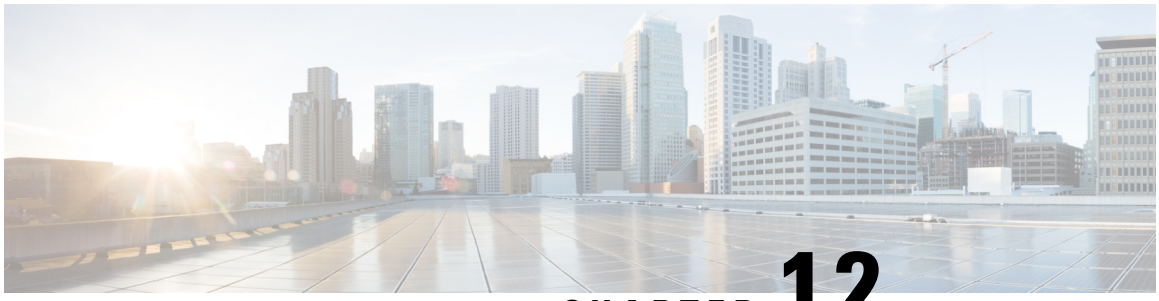
Step 5 Click **Launch**.

Step 6 Select an existing key pair or create a new key pair.

Step 7 Click **Launch Instances**.

Step 8 Click **View Launch** and follow the prompts.

Step 9 Go to **Instance** > **More** > **Operations and Troubleshooting** > **Get Instance System Logs**.



CHAPTER 12

Deploy the Firewall Management Center Virtual on Hyper-V

Microsoft Hyper-V is Microsoft's hardware virtualization platform, also termed as a *hypervisor*. Hyper-V enables administrators to make better use of hardware by using the same physical server to run multiple virtual machines.

Virtual machines provide more flexibility, save cost, and are a more efficient way to use hardware than running only one operating system on physical hardware.

This chapter contains the following sections:

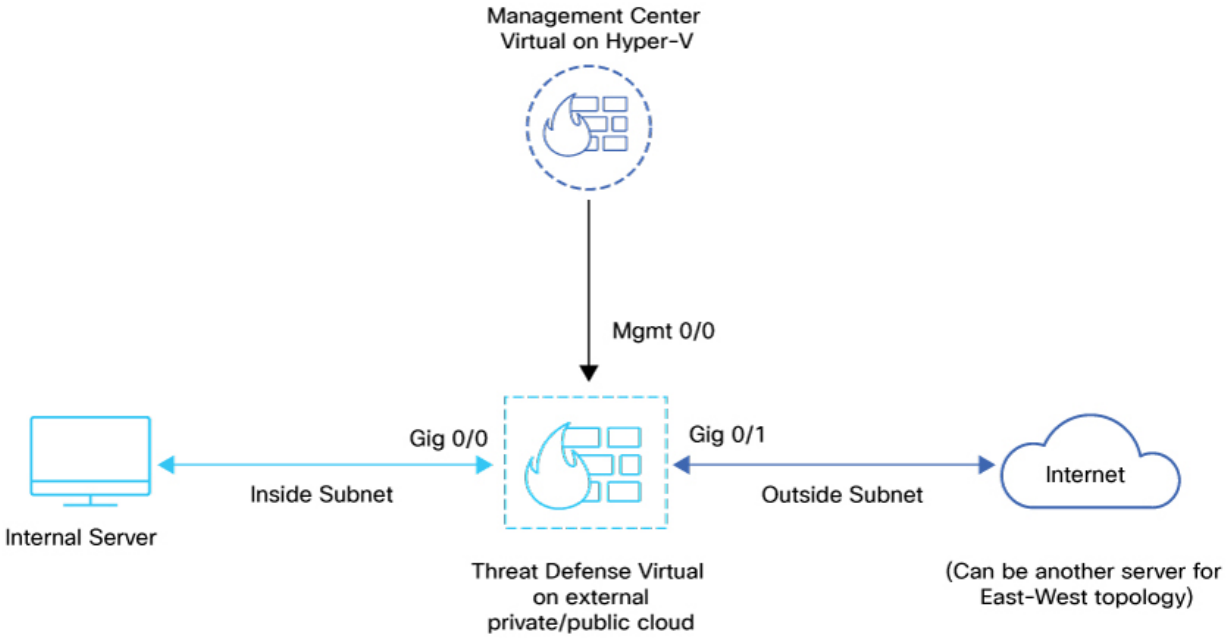
- Overview, on page 129
- Sample Topology of Management Center Virtual on Hyper-V, on page 130
- Supported Windows Server for Management Center Virtual, on page 130
- Guidelines and Limitations for Management Center Virtual on Hyper-V, on page 130
- Licenses for Deployment of Management Center Virtual on Hyper-V, on page 131
- Prerequisites for Deployment of Management Center Virtual on Hyper-V, on page 131
- Deploy the Management Center Virtual, on page 131
- Verify the Deployment, on page 134
- Access First Boot Logs, on page 134
- Shut Down Management Center Virtual, on page 135
- Reboot Management Center Virtual, on page 135
- Delete Management Center Virtual, on page 135
- Troubleshooting, on page 136

Overview

Management Center Virtual is deployed on Hyper-V by using a VHD image available on Cisco.com. Basic VM control features such as Console Access, Stop/Restart, IPv4, and IPv6 support for management interface are supported. The initial configuration is done using a day-0 configuration script. High availability is supported.

Sample Topology of Management Center Virtual on Hyper-V

In this sample topology, Management Center Virtual is connected to the management port of the threat defense virtual deployed on an external private or public cloud. The Threat Defense Virtual is connected to both the internet and an internal server. The internet can also be another server in an east-west traffic flow topology.



Supported Windows Server for Management Center Virtual

Management Center Virtual 25 is supported on Windows Server 2019 and Windows Server 2025 Standard Edition. The minimum resource requirements for the Management Center Virtual are given below:

- CPU: 4 vCPUs
- RAM: 28 GB (recommended 32 GB)
- Disk storage: 250 GB
- Minimum number of interfaces: 1

Guidelines and Limitations for Management Center Virtual on Hyper-V

- Management Center Virtual deployed on Hyper-V can be used to manage threat defense virtual clusters that are deployed on other public or private clouds. However, to manage threat defense virtual clusters deployed on public cloud, you must manually register the cluster with Management Center Virtual. See Add the Cluster to the Management Center (Manual Deployment).

- Cloning is not supported.

Licenses for Deployment of Management Center Virtual on Hyper-V

The following license types are supported:

- BYOL
  - Smart License
  - Specific License Reservation (SLR)
  - Universal Permanent License Registration (PLR)
- Evaluation License

Prerequisites for Deployment of Management Center Virtual on Hyper-V

- Microsoft Windows Server with Hyper-V role and Hyper-V Manager installed. See Get started with Hyper-V on Windows Server.
- Download the Management Center Virtual compressed VHD image from Cisco.com.
- BYOL license
- New virtual switch (vSwitch) and virtual machine (VM)

Deploy the Management Center Virtual

Perform the procedures given below to deploy the Management Center Virtual on Hyper-V.

Download Management Center Virtual VHD Image

Download the Management Center Virtual compressed VHD image from the Cisco Download Software page to your local machine:

1. Navigate to **Products > Security > Firewalls > Firewall Management > Secure Firewall Management Center Virtual**
2. Click **Firepower Management Center Software** and download the required VHD image. For example, Cisco_Secure_FW_Mgmt_Center_Virtual_Azure-7.4.0- xxxx.vhd.tar.

Prepare Day 0 Configuration File

Preparing a Day-0 configuration file before launching the Management Center Virtual is recommended to automate the initial setup. This initial configuration is placed into a text file named **day0-config** on your local machine, and is converted to a day0.iso file that is mounted and read on first boot.

Note While the day0.iso file must be available during first boot for automated configuration, deployment can proceed without it. If omitted, manual configuration is required after launch.

Specify the following parameters in the Day-0 configuration file:

- The End User License Agreement (EULA) acceptance.
- A host name for the system.
- A new administrator password for the admin account.
- Network settings that allow the appliance to communicate on your management network.

Note We have used Linux in the following example, but there are similar utilities for Windows.

Procedure

Step 1 Enter the CLI configuration for Management Center Virtual in a text file called **day0-config**. Add the network settings and information about managing Management Center Virtual.

```
{
"EULA": "accept",
"Hostname": "virtual731265",
"AdminPassword": "r2M$9^Uk69##",
"DNS1": "208.67.222.222",
"DNS2": "208.67.222.222",
"IPv4Mode": "Manual",
"IPv4Addr": "10.10.0.92",
"IPv4Mask": "255.255.255.224",
"IPv4Gw": "10.10.0.65",
"IPv6Mode": "Manual",
"IPv6Addr": "2001:420:5440:2010:600:0:45:45",
"IPv6Mask": "112",
"IPv6Gw": "2001:420:5440:2010:600:0:45:1"
}
```

Step 2 Generate the virtual CD-ROM by converting the text file to an ISO file:

```
/usr/bin/genisoimage -r -o day0.iso day0-config
```

or

```
/ usr/bin/mkisofs -r -o day0.iso day0-config
```

Create a New Virtual Switch

Perform this procedure to create a new virtual switch (vSwitch).

Procedure

Step 1 On the Hyper-V Manager **Actions** tab, click **Virtual Switch Manager**.

Step 2 Click **Virtual Switches** > **New virtual network switch**.

Step 3 In the **Create virtual switch** window, select **External**.

Step 4 Click **Create Virtual Switch**.

Step 5 In the **Virtual Switch Properties** window, enter a **Name** for the virtual switch.

Step 6 Create an external or internal vSwitch.

- To create an external vSwitch, select **External network** and the required physical adaptor from the drop-down list.
- To create an internal vSwitch, select **Internal network** or **Private network**.

Step 7 Under **VLAN ID**, check the check box next to **Enable virtual LAN identification for management operating system**.

Step 8 Click **OK**.

Create a New Virtual Machine

Perform this procedure to create a new VM.

Procedure

Step 1 On the Hyper-V Manager, click **Action** > **New** > **Virtual Machine**

Step 2 Click **Next** on the **New Virtual Machine Wizard** dialog box.

Step 3 Enter a **Name** for the VM and click **Next**.

Step 4 Choose **Generation 1** and click **Next**.

Step 5 Specify the amount of **Startup Memory** or RAM, in MB, that has to be allocated for the VM (Minimum is 28672 MB, recommended is 32768 MB)

Step 6 Choose the required vSwitch **Connection** from the drop-down list.

Step 7 Choose **Use an existing virtual hard disk** and click **Browse** to choose the downloaded Management Center Virtual VHD image.

Step 8 Click **Finish** to create the VM.

Step 9 After creating the virtual machine, it is important to increase the number of virtual processors (vCPU) for the virtual machine. By default, its value is set to *1*.

a) On the **Hyper-V Manager**, right-click the virtual machine that you have created and click **Settings**.
The virtual machines' **Settings** window is displayed.

b) Click **Processor** under **Hardware** on the left-pane.

The **Processor** dialog box is displayed on the right-pane.

c) In the **Number of virtual processors:** field, set the value to **4**.

Note We recommend to set the vCPUs (virtual processors) value to *8* for optimal performance. Note that a virtual machine requires a minimum of *4* vCPUs (virtual processors).

For more information on minimum resource requirement, see Supported Windows Server for Management Center Virtual, on page 130

d) Click **OK**.

Verify the Deployment

Run the **show version** command on the serial console to ensure that management center virtual is deployed on Hyper-V.

```
rm-Production login: admin
Password:

Copyright 2004-2022, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Firepower Extensible Operating System (FX-OS) v82.14.0 (build 205)
Cisco Secure Firewall Management Center for Hyper-V v7.4.0 (build 1493)

> show version
-----------------[ rm-Production ]-----------------
Model                     : Secure Firewall Management Center for Hyper-V (66) V
ersion 7.4.0 (Build 1493)
UUID                      : 3f775634-7f7d-11ed-b8f5-0c0e70c660f3
Rules update version      : 2022-01-06-001-vrt
LSP version               : lsp-rel-20221214-1542
VDB version               : 361
----------------------------------------------------
```

Access First Boot Logs

To access the first boot logs, perform this procedure before turning on the VM that you created on the Hyper-V Manager.

Procedure

Step 1 On the Hyper-V Manager, select the newly created VM, and click **Settings** in the **Actions** section on the right side of the window.

Step 2 In the **Hardware** section, click **COM1** and choose **Named Pipe**.

Step 3 Enter a **Pipe name**. For example, **virtual1**. Note the **Named pipe path**.

Step 4 Click **Apply** and then click **OK**.

Step 5 Click the VM created by you and click **Start** in the **Actions** window on the right side of the window. The **State** of the VM should now change from **Starting** to **Running**.

Step 6 You must now connect the named pipe created by you to a serial client, such as **PuTTY**.

Step 7 Go to your local host and bring up the **PuTTY** window.

Step 8 Enter the **Named pipe path** that you noted down earlier in the **Serial line** field.

For example, \\.*pipe**virtual1*.

Step 9 Click **Open**. You can now see the first boot logs on the **PuTTY** window.

Shut Down Management Center Virtual

On the Hyper-V Manager, right-click the VM that you want to shut down, and click **Turn Off**.

Reboot Management Center Virtual

Run the **sudo reboot** command in **expert** mode on the Management Center Virtual CLI to initiate a graceful reboot:

```
Cisco Firepower Extensible Operating System (FX-OS) v82.14.0
(build 205)
Cisco Secure Firewall Management Center for Hyper-V v7.4.0
(build 1493)
> expert
admin@hyperv-automation:~$ sudo reboot
```

Alternatively, you can also go to Hyper-V Manager, right-click the VM that you want to shut down, and click **Turn Off**.

Delete Management Center Virtual

After the VM is shut down, right-click the VM, and click **Delete**.

Note Deleting does not delete the disk attached to the VM. You must manually delete that disk.

Troubleshooting

- Issue - Unable to start VM, could not initialize memory

  Scenario - This issue occurs when the disk space is not enough to initialize the VM.

  Workaround - Clear up space on the disk where the VHD file is located.

- Issue - Unable to provision or start the VM; failed to open the attachment.

  Scenario - This issue occurs when another VM is using the same image as the new VM

  Workaround - Delete the old VM.

- Issue - Failed to start the VM, not enough system memory

  Scenario - This issue occurs when not enough RAM is available on the host operating system to provision the configured memory to the VM.

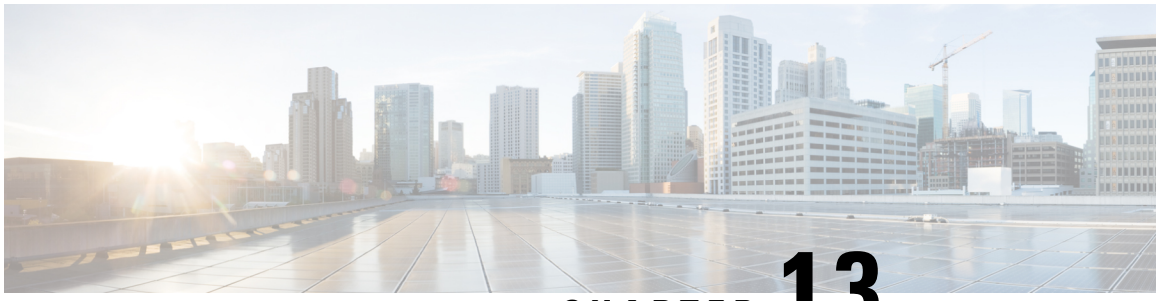
  Workaround - Ensure that the required RAM is available on the host operating system.

- Issue - Unable to SSH to Management Center Virtual or load the Management Center Virtual UI from an external host.

  Workaround - Allow port 22 (SSH), 443 (HTTPS), 80 (HTTP) in inbound and outbound rules in the Windows Firewall.

- Issue - Device is unable to access the internet.

  Workaround - If the device is using an external vSwitch, ensure that the gateway of the VLAN is properly configured.



CHAPTER 13

Firewall Management Center Virtual Initial Setup

This chapter describes the initial setup process you need to perform after you deploy the Firewall Management Center Virtual appliance.

- Firewall Management Center Initial Setup Using the CLI for Versions 6.5 and Later, on page 137
- Perform Initial Setup at the Web Interface for Versions 6.5 and Later, on page 140
- Review Automatic Initial Configuration for Versions 6.5 and Later, on page 144

Firewall Management Center Initial Setup Using the CLI for Versions 6.5 and Later

After you deploy an Firewall Management Center Virtual, you can access the appliance console for initial setup.You can perform initial setup using the CLI as an alternative to using the web interface. You must complete an Initial Configuration Wizard that configures the new appliance to communicate on your trusted management network. The wizard requires that you accept the end user license agreement (EULA) and change the administrator password.

Before you begin

- Be sure you have the following information needed for the Firewall Management Center Virtual to communicate on your management network:
  - An IPv4 management IP address.

    The Firewall Management Center 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 Firewall Management Center MAC address. In scenarios where no DHCP is available, the Firewall Management Center interface uses the IPv4 address 192.168.45.45.
  - A network mask and a default gateway (if not using DHCP).

Procedure

Step 1 Log into the Firewall Management Center Virtual at the console using **admin** as the username and **Admin123** as the password for the **admin** account. Note that the password is case-sensitive.

Step 2 When prompted, press **Enter** to display the End User License Agreement (EULA).

Step 3 Review the EULA. When prompted, enter **yes**, **YES**, or press **Enter** to accept the EULA.



Important You cannot proceed without accepting the EULA. If you respond with anything other than **yes**, **YES**, or **Enter**, the system logs you out.

Step 4 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 system prompts for a new password, enter a new password complying with the restrictions displayed, and enter the same password again when the system prompts for confirmation.



Note The Firewall Management Center compares your password against a password cracking dictionary that checks not only for many English dictionary words but also other character strings that could be easily cracked with common password hacking techniques. For example, the initial configuration script may reject passwords such as "abcdefg" or "passw0rd".



Note On completion of the initial configuration process the system sets the passwords for the two **admin** accounts (one for web access and the other for CLI access) to the same value, complying with the strong password requirements described in the *Cisco Secure Firewall Management Center Administration Guide* for your version. If you change the password for either **admin** account thereafter, they will no longer be the same, and the strong password requirement can be removed from the web interface **admin** account.

Step 5 Answer the prompts to configure network settings.

When following the prompts, for multiple-choice questions, your options are listed in parentheses, such as **(y/n)**. Defaults are listed in square brackets, such as **[y]**. Note the following when responding to prompts:

- Press **Enter** to accept the default.
- For hostname, supply a fully qualified domain name (`<hostname>.<domain>`) or host name. This field is required.
- 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.
- If you choose to configure IPv4 manually, the system prompts for IPv4 address, netmask, and default gateway.
- Configuring a DNS server is optional; to specify no DNS server enter **none**. Otherwise specify IPv4 addresses for one or two DNS servers. If you specify two addresses, separate them with a comma. (If you specify more than two DNS servers, the system ignores the additional entries.) If your Firewall Management Center does not have internet access you cannot use a DNS outside of your local network.



Note If you are using an evaluation license, specifying DNS is optional at this time, but DNS is required to use permanent licenses for your deployment.

- You must enter the fully qualified domain name or IP address for at least one NTP server reachable from your network. (You may not specify FQDNs for NTP servers if you are not using DHCP.) You may specify two servers (a primary and a secondary); separate their information with a comma. (If you specify more than two DNS servers, the system ignores the additional entries.) If your Firewall Management Center does not have internet access you cannot use an NTP server outside of your local network.

Example:

```
Enter a hostname or fully qualified domain name for this system [firepower]: fmc
Configure IPv4 via DHCP or manually? (dhcp/manual) [DHCP]: manual
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.0.66
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.224
Enter the IPv4 default gateway for the management interface [ ]: 10.10.0.65
Enter a comma-separated list of DNS servers or 'none' [CiscoUmbrella]: 208.67.222.222,208.67.220.220
Enter a comma-separated list of NTP servers [0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org]:
```

Step 6 The system displays a summary of your configuration selections. Review the settings you have entered.

Example:

```
Hostname:                           fmc
IPv4 configured via:                manual configuration
Management interface IPv4 address:  10.10.0.66
Management interface IPv4 netmask:  255.255.255.224
Management interface IPv4 gateway:  10.10.0.65
DNS servers:                        208.67.222.222,208.67.220.220
NTP servers:                        0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org
```

Step 7 The final prompt gives you the opportunity to confirm the settings.

- If the settings are correct, enter **y** and press **Enter** to accept the settings and continue.
- If the settings are incorrect, enter **n** and press **Enter**. The system prompts for the information again, beginning with hostname.

Example:

```
Are these settings correct? (y/n) y
If your networking information has changed, you will need to reconnect.

Updated network configuration.
```

Step 8 After you have accepted the settings, you can enter **exit** to exit the Firewall Management Center CLI.

What to do next

- You can connect to the Firewall Management Center Virtual web interface using the network information you have just configured.
- Review the weekly maintenance activites the Firewall Management Center configures automatically as a part of the initial configuration process. These activities are designed to keep your system up-to-date and your data backed up. See Review Automatic Initial Configuration for Versions 6.5 and Later, on page 144 .

- You can configure the Firewall Management Center for IPv6 addressing after completing the initial setup using the web interface as described in the *Cisco Secure Firewall Management Center Device Configuration Guide* for your version.

Perform Initial Setup at the Web Interface for Versions 6.5 and Later

After you deploy a Firewall Management Center Virtual, you can perform initial setup using HTTPS at the appliance web interface.

When you log into the Firewall Management Center web interface for the first time, the Firewall Management Center presents an Initial Configuration Wizard to enable you to quickly and easily configure basic settings for the appliance. This wizard consists of three screens and one pop-up dialog box:

- The first screen forces you to change the password for the **admin** user from the default value of **Admin123**.
- The second screen presents the End User License Agreement (EULA), which you are required to accept before using the appliance.
- The third screen allows you to change network settings for the appliance management interface. This page is prepopulated with current settings, which you may change.
- The wizard performs validation on the values you enter on this screen to confirm the following:
  - Syntactical correctness
  - Compatibility of the entered values (for instance, compatible IP address and gateway, or DNS provided when NTP servers are specified using FQDNs)
  - Network connectivity between the Firewall Management Center Virtual and the DNS and NTP servers

  The wizard displays the results of these tests in real time on the screen, which allows you to make corrections and test the viability of your configuration before clicking **Finish** at the bottom of the screen. The NTP and DNS connectivity tests are nonblocking; you can click **Finish** before the wizard completes the connectivity tests. If the system reports a connectivity problem after you click **Finish**, you cannot change the settings in the wizard, but you can configure these connections using the web interface after completing the initial setup.

  The system does not perform connectivity testing if you enter configuration values that would result in cutting off the existing connection between the Firewall Management Center Virtual and the browser. In this case the wizard displays no connectivity status information for DNS or NTP.
- After you have completed the three wizard screens, a pop-up dialog box appears that offers you the opportunity to (optionally) quickly and easily set up Smart Licensing.

When you have completed the Initial Configuration Wizard and completed or dismissed the Smart Licensing dialog, the system displays the device management page, described in “Device Management” in the *Cisco Secure Firewall Management Center Device Configuration Guide* for your version.

Before you begin

- Be sure you have the following information needed for the Firewall Management Center to communicate on your management network:
  - An IPv4 management IP address.

    The Firewall Management Center 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 Firewall Management Center MAC address. In scenarios where no DHCP is available, the Firewall Management Center interface uses the IPv4 address 192.168.45.45.
  - A network mask and a default gateway (if not using DHCP).
- If you are not using DHCP, configure a local computer with the following network settings:
  - IP address: 192.168.45.2
  - Netmask: 255.255.255.0
  - Default gateway: 192.168.45.1

  Disable any other network connections on this computer.

Procedure

Step 1 Use a web browser to navigate to the Firewall Management Center Virtual's IP address: *https://<Management Center-IP>*.

The login page appears.

Step 2 Log into the Firewall Management Center Virtual using **admin** as the username and **Admin123** as the password for the admin account. (The password is case-sensitive.)

Step 3 At the **Change Password** screen:

a) (Optional) Check the **Show password** check box to see the password while using this screen.

b) (Optional) Click the **Generate Password** button to have the system create a password for you that complies with the listed criteria. (Generated passwords are nonmnemonic; take careful note of the password if you choose this option.)

c) To set a password of your choosing, enter a new password in the **New Password** and **Confirm Password** text boxes.

The password must comply with the criteria listed in the dialog.

Note The Firewall Management Center compares your password against a password cracking dictionary that checks not only for many English dictionary words but also other character strings that could be easily cracked with common password hacking techniques. For example, the initial configuration script may reject passwords such as "abcdefg" or "passw0rd".

Note On completion of the initial configuration process the system sets the passwords for the two **admin** accounts (one for web access and the other for CLI access) to the same value. The password must comply with the strong password requirements described in the *Cisco Secure Firewall Management Center Administration Guide* for your version. If you change the password for either **admin** account thereafter, they will no longer be the same, and the strong password requirement can be removed from the web interface **admin** account.

d) Click **Next**.

Once you click **Next** on the **Change Password** screen and the wizard has accepted the new **admin** password, that password is in effect for both the web interface and CLI **admin** accounts even if you do not complete the remaining wizard activities.

Step 4 At the **User Agreement** screen, read the EULA and click **Accept** to proceed.

If you click **Decline** the wizard logs you out of the Firewall Management Center Virtual.

Step 5 Click **Next**.

Step 6 At the **Change Network Settings** screen:

a) Enter a **Fully Qualified Domain Name**. If default value is shown, you may use that if it is compatible with your network configuration. Otherwise, enter a fully qualified domain name (syntax `<hostname>.<domain>`) or hostname.

b) Choose the boot protocol for the **Configure IPv4** option, either **Using DHCP** or **Using Static/Manual**.

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.

c) Accept the displayed value, if one is shown, for **IPv4 Address** or enter a new value. Use dotted decimal form (for example, 192.168.45.45).

Note If you change the IP address during initial configuration, you need to reconnect to the Firewall Management Center using the new network information.

d) Accept the displayed value, if one is shown, for **Network Mask** or enter a new value. Use dotted decimal form (for example, 255.255.0.0).

Note If you change the network mask during initial configuration, you need to reconnect to the Firewall Management Center using the new network information.

e) You can accept the displayed value, if one is shown, for **Gateway** or enter a new default gateway. Use dotted decimal form (for example, 192.168.0.1).

Note If you change the gateway address during initial configuration, you may need to reconnect to the Firewall Management Center using the new network information.

f) (Optional) For **DNS Group** you can accept the default value, **Cisco Umbrella DNS**.

To change the DNS settings, choose **Custom DNS Servers** from the drop-down list, and enter IPv4 addresses for the **Primary DNS** and **Secondary DNS**. If your Firewall Management Center does not have internet access you cannot use a DNS outside of your local network. Configure no DNS Server by choosing **Custom DNS Servers** from the drop-down list and leaving the **Primary DNS** and **Secondary DNS** fields blank.

Note If you use FQDNs rather than IP addresses to specify NTP servers, you must specify DNS at this time. If you are using an evaluation license DNS is optional, but DNS is required to use permanent licenses for your deployment.

g) For **NTP Group Servers** you can accept the default value, **Default NTP Servers**. In this case the system uses **0.sourcefire.pool.ntp.org** as the primary NTP server, and **1.sourcefire.pool.ntp.org** as the secondary NTP server.

To configure other NTP servers, choose **Custom NTP Group Servers** from the drop-down list and enter the FQDNs or IP addresses of one or two NTP servers reachable from your network. If your Firewall Management Center does not have internet access you cannot use an NTP server outside of your local network.

Note If you change network settings during initial configuration, you need to reconnect to the Firewall Management Center using the new network information.

Step 7 Click **Finish**.

The wizard performs validation on the values you enter on this screen to confirm syntactical correctness, compatibility of the entered values, and network connectivity between the Firewall Management Center and the DNS and NTP servers. If the system reports a connectivity problem after you click **Finish**, you cannot change the settings in the wizard, but you can configure these connections using the Firewall Management Center web interface after completing the initial setup.

What to do next

- The system displays a pop-up dialog box that offers you the opportunity to quickly and easily set up Smart Licensing. Using this dialog box is optional; if your Firewall Management Center Virtual will be managing Firewall Threat Defenses and you are familiar with Smart Licensing, use this dialog. Otherwise dismiss this dialog and refer to ”Licensing” in the *Cisco Secure Firewall Management Center Administration Guide* for your version.
- Review the weekly maintenance activites the Firewall Management Center configures automatically as a part of the initial configuration process. These activities are designed to keep your system up-to-date and your data backed up. See Review Automatic Initial Configuration for Versions 6.5 and Later, on page 144 .

- When you have completed the Initial Configuration Wizard and completed or dismissed the Smart Licensing dialog, the system displays the device management page, described in the *Cisco Secure Firewall Management Center Device Configuration Guide*.
- You can configure the Firewall Management Center for IPv6 addressing after completing the initial setup using the web interface as described in the *Cisco Secure Firewall Management Center Device Configuration Guide* for your version.

Review Automatic Initial Configuration for Versions 6.5 and Later

As a part of initial configuration (whether performed through the Initial Configuration Wizard or through the CLI), the Firewall Management Center automatically configures maintenance tasks to keep your system up-to-date and your data backed up.

These tasks are scheduled in UTC, which means that when they occur *locally* depends on the date and your specific location. Also, because tasks are scheduled in UTC, they do not adjust for daylight saving time, summer time, or any such seasonal adjustments that you may observe in your location. If you are affected, scheduled tasks occur one hour "later" in the summer than in the winter, according to local time.



Note We *strongly* recommend you review the auto scheduled configurations, confirm that the Firewall Management Center has established them successfully, and adjust them if necessary.

- Weekly GeoDB Updates

  The Firewall Management Center automatically schedules GeoDB updates to occur each week at the same randomly selected time. You can observe the status of this update using the web interface Message Center. You can see the configuration for this automatic update in the web interface under **System** > **Updates** > **Geolocation Updates**>**Recurring Geolocation Updates**. If the system fails to configure the update and your Firewall Management Center has internet access, we recommend you configure regular GeoDB updates as described in the *Cisco Secure Firewall Management Center Administration Guide* for your version.

- Weekly Firewall Management Center Software Updates

  The Firewall Management Center automatically schedules a weekly task to download the latest software for the Firewall Management Center and its managed devices. This task is scheduled to occur between 2 and 3 AM UTC on Sunday mornings; depending on the date and your specific location this can occur any time from Saturday afternoon to Sunday afternoon local time. You can observe the status of this task using the web interface Message Center. You can see the configuration for this task in the web interface under **System** > **Tools** > **Scheduling**. If the task scheduling fails and your Firewall Management Center has internet access, we recommend you schedule a recurring task for downloading software updates as described in the *Cisco Secure Firewall Management Center Administration Guide* for your version.

  This task only downloads software patch and hotfix updates for the version your appliances are currently running; it it your responsibility to install any updates this task downloads. See the *Cisco Firewall Management Center Upgrade Guide* for more information.

- Weekly Firewall Management Center Configuration Backup

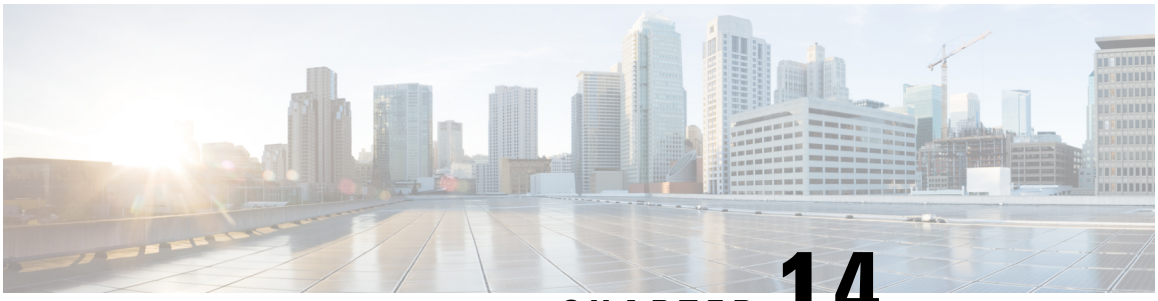
The Firewall Management Center automatically schedules a weekly task to perform a locally-stored configuration-only backup at 2 AM UTC on Monday mornings; depending on the date and your specific location this can occur any time from Saturday afternoon to Sunday afternoon local time. You can observe the status of this task using the web interface Message Center. You can see the configuration for this task in the web interface under **System** > **Tools** > **Scheduling**. If the task scheduling fails, we recommend you schedule a recurring task to perform backups as described in the *Cisco Secure Firewall Management Center Administration Guide* for your version.

- Vulnerability Database Update

  In Versions 6.6+, the Firewall Management Center downloads and installs the latest vulnerability database (VDB) update from the Cisco support site. This is a one-time operation. You can observe the status of this update using the web interface Message Center. To keep your system up to date, if your Firewall Management Center has internet access, we recommend you schedule tasks to perform automatic recurring VDB update downloads and installations as described in the *Cisco Secure Firewall Management Center Administration Guide* for your version.

- Daily Intrusion Rule Update

  In Versions 6.6+, the Firewall Management Center configures a daily automatic intrusion rule update from the Cisco support site. The Firewall Management Center deploys automatic intrusion rule upates to affected managed devices when it next deploys affected policies. You can observe the status of this task using the web interface Message Center. You can see the configuration for this task in the web interface under **System** > **Updates** > **Rule Updates**. If configuring the update fails and your Firewall Management Center has internet access, we recommend you configure regular intrusion rule updates as described in the *Cisco Secure Firewall Management Center Administration Guide* for your version.



CHAPTER 14

Firewall Management Center Virtual Initial Administration and Configuration

After you complete the initial setup process for the Firewall Management Center Virtual and verify its success, we recommend that you complete various administrative tasks that make your deployment easier to manage. You should also complete any tasks you skipped during the initial setup, such as licensing. For detailed information on any of the tasks described in the following sections, as well as information on how you can begin to configure your deployment, see the complete Secure Firewall Management Center Configuration Guide for your version.

- Individual User Accounts, on page 147
- Device Registration, on page 148
- Health and System Policies, on page 148
- Software and Database Updates, on page 148
- Troubleshooting, on page 149

Individual User Accounts

After you complete the initial setup, the only web interface user on the system is the **admin** user, which has the Administrator role and access. Users with that role have full menu and configuration access to the system. We recommend that you limit the use of the **admin** account (and the Administrator role) for security and auditing reasons. In the Firewall Management Center Virtual GUI, manage user accounts on the **System** > **Users** > **User** page.

Note The **admin** accounts for accessing the Firewall Management Center Virtual using the shell and accessing the Firewall Management Center Virtual using the web interface are not the same, and may use different passwords.

Creating a separate account for each person who uses the system allows your organization not only to audit actions and changes made by each user, but also to limit each person's associated user access role or roles. This is especially important on the Firewall Management Center Virtual, where you perform most of your configuration and analysis tasks. For example, an analyst needs access to event data to analyze the security of your network, but may not require access to administrative functions for the deployment.

The system includes ten predefined user roles designed for a variety of administrators and analysts using the web interface. You can also create custom user roles with specialized access privileges.

Device Registration

The Firewall Management Center can manage any device, physical or virtual, currently supported by the system:

- Firewall Threat Defense—Provides a unified next-generation firewall and next-generation IPS device.
- Firewall Threat Defense Virtual—A 64-bit virtual device that is designed to work in multiple hypervisor environments, reduce administrative overhead, and increase operational efficiency.
- Cisco ASA with FirePOWER Services (or an ASA FirePOWER module)—Provides the first-line system policy and passes traffic to the system for discovery and access control. However, you cannot use the Firewall Management Center web interface to configure ASA FirePOWER interfaces. Cisco ASA with FirePOWER Services has a software and CLI unique to the ASA platform that you can use to install the system and to perform other platform-specific administrative tasks.
- 7000 and 8000 Series appliances—Physical devices purpose-built for the system. 7000 and 8000 Series devices have a range of throughputs, but share most of the same capabilities. In general, 8000 Series devices are more powerful than 7000 Series devices; they also support additional features such as 8000 Series fastpath rules, link aggregation, and stacking. You must configure remote management on the device before you can register the device to the Firewall Management Center.
- NGIPSv—A 64-bit virtual device deployed in the VMware VSphere environment. NGIPSv devices do not support any of the system's hardware-based features such as redundancy and resource sharing, switching, and routing.

To register managed devices to the Firewall Management Center use the **Devices** > **Device Management** page on the Firewall Management Center GUI; see the device management information in the Secure Firewall Management Center Configuration Guide for your version.

Health and System Policies

By default, all appliances have an initial system policy applied. The system policy governs settings that are likely to be similar for multiple appliances in a deployment, such as mail relay host preferences and time synchronization settings. We recommend that you use the Firewall Management Center to apply the same system policy to itself and all the devices it manages.

By default, the Firewall Management Center also has a health policy applied. A health policy, as part of the health monitoring feature, provides the criteria for the system to continuously monitor the performance of the appliances in your deployment. We recommend that you use the Firewall Management Center to apply a health policy to all the devices it manages.

Software and Database Updates

You should update the system software on your appliances before you begin any deployment. We recommend that all the appliances in your deployment run the most recent version of the system. If you are using them in your deployment, you should also install the latest intrusion rule updates, VDB, and GeoDB.

Caution Before you update any part of the system, you must read the release notes or advisory text that accompanies the update. The release notes provide important information, including supported platforms, compatibility, prerequisites, warnings, and specific installation and uninstallation instructions.

If your Firewall Management Center is running Versions 6.5+:

As a part of configuration the Firewall Management Center establishes the following activities to keep your system up-to-date and your data backed up:

- Weekly automatic GeoDB updates
- A weekly task to download the latest software for the Firewall Management Center and its managed devices

Important This task only downloads software updates to the Firewall Management Center. It is your responsibility to install any updates this task downloads. See the *Cisco Secure Firewall Management Center Upgrade Guide* for more information.

- A weekly task to perform a locally-stored configuration-only the Firewall Management Center backup

If your Firewall Management Center is running Versions 6.6+, as a part of initial configuration the Firewall Management Center downloads and installs the latest vulnerability (VDB) update from the Cisco support site. This is a one-time operation.

You can observe the status of these activities using the web interface Message Center. If the system fails to configure any of these activities and your Firewall Management Center has internet access, we recommend you configure these activities yourself as described in the *Secure Firewall Management Center Configuration Guide* for your version.

Troubleshooting

This section provides you with some basic troubleshooting steps related to your Firewall Management Center Virtual deployment on your virtual machine.

SSH Connection Failure

The Firewall Management Center Virtual is fully operational, with the user interface and console connection functioning correctly, except for the SSH connection. In certain scenarios, the SSH host key files might become corrupted during the initial boot of the Firewall Management Center Virtual, resulting in SSH connection failures.

You can check for the following indications that suggest an SSH connection failure:

1. A disk I/O error might occur during the initial boot of the Firewall Management Center Virtual, specifically when the SSH daemon (sshd) is starting. This results in the SSH key files (ssh_host* files generated by sshd) being empty.

```
ls -lrt /etc/ssh total 16

-rw-r--r-- 1 root root 1746 Jan 17 23:31 ssh_config-openssh
-rw-r--r-- 1 root root 6027 Jan 17 23:42 sshd_config
```

```
-rw-r--r-- 1 root root 1293 Jan 17 23:42 ssh_config
-rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_dsa_key
-rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_dsa_key.pub
-rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_ecdsa_key
-rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_ecdsa_key.pub
-rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_ed25519_key
-rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_ed25519_key.pub
-rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_rsa_key
-rw-r--r-- 1 root root    0 Jan 27 06:37 ssh_host_rsa_key.pub
```

2. For the disk I/O issue, you can check the `/var/log/messages` file, which may contain erroneous data (indicating an I/O error) around the same timestamp when the SSH key files were generated.

To resolve the SSH failure that might occur during the initial boot of Firewall Management Center Virtual, as described above, you should perform the following steps:

1. Log in to Firewall Management Center Virtual.
2. Run the **sudo reboot** command in **expert** mode on the Firewall Management Center Virtual CLI to initiate a graceful reboot.
3. Run the following command to remove the empty SSH key files:

```
cd /etc/ssh/
rm ssh_host*
```

4. Run the following command to restart the `sshd` service to regenerate the SSH key files properly.

```
/etc/rc.d/init.d/sshd stop
/etc/rc.d/init.d/sshd start
```

Note Follow this workaround steps only if you are certain that the SSH key files are empty. If you are uncertain, it is advisable to submit a TAC case for further investigation.