Deploy the Management Center Virtual On the Microsoft Azure Cloud

You can deploy the management center virtual as a virtual machine on the Microsoft Azure public cloud.

Important The management center virtual is supported on Microsoft Azure starting with Cisco software version 6.4 and later.

Overview

You deploy the management center virtual in Microsoft Azure using a solution template available in the Azure Marketplace. When you deploy the 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 management center virtual, allowing you to login to the management center virtual web interface after first boot.

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

The management center virtual platform has introduced a new memory check during upgrade. The 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 management center virtual deployments (AWS, Azure) are fully deprecated. You cannot create new management center virtual instances using them, even for earlier versions. You can continue running existing instances. See Table 1: Azure Supported Instances for the Management Center Virtual, on page 2.

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

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

The following table summarizes the Azure instances types that the management center virtual supports; those that Versions 6.5.x and earlier support, and those that Version 6.6.0+ support.

Table 1: Azure Supported Instances for the Management Center Virtual

Platform	Version 6.6.0+	Version 6.5.x and earlier*
Management Center Virtual	Standard_D4_v2: 8 vCPUs, 28 GB	Standard_D3_v2: 4 vCPUs, 14 GB
	—	Standard_D4_v2: 8 vCPUs, 28 GB
	*Note that the management center virtual will no longer support the Standard_D3_v2 instance after Version 6.6.0 is released. Beginning with Version 6.6.0, you must deploy the management center virtual (any version) using an instance with at least 28 GB RAM. See Resizing Instances, on page 2.	

Table 2: Azure Supported Instance for the FMCv300

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

Deprecated Instances

You can continue running your current Version 6.5.x and earlier the management center virtual deployments using Standard_D3_v2, but you will not be able to launch new management center virtual deployments (any version) using this instance.

Resizing Instances

Because the upgrade path from any earlier version of 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 instance type to Standard_D4_v2 (see Table 1: Azure Supported Instances for the Management Center Virtual, on page 2).

You can use the Azure portal or PowerShell to resize your instance. 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 instance, see the Azure documentation “Resize a Windows VM” (https://docs.microsoft.com/en-us/azure/virtual-machines/windows/resize-vm).

Prerequisites

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

Verify the following before you deploy the 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 management center virtual, and choose the “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 Instances
  - 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 management center virtual in the Azure public marketplace supports the Bring Your Own License (BYOL) model. For the 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 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 management center virtual VM. These are not graceful shutdown mechanisms and can lead to database corruption.

Use the **System** > **Configuration** options available from the management center virtual's Web interface to shut down or restart the virtual appliance.

Use the `shutdown` and `restart` commands from the 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 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 management center virtual HA, 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 threat defense feature license entitlement for each threat defense device has no change regardless of the 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 management center virtual HA pair, the extra management center virtual license entitlement is released, and you need only one entitlement for each 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 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 management center virtual in Azure the following resources are created:

- The management center virtual Machine with a single interface (requires a new or an existing virtual network with 1 subnet).
- A Resource Group.

  The 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 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 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 Management Center Virtual

You can deploy the 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 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 6.

- **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 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 management center virtual in a single, coordinated operation.

Deploy from Azure Marketplace Using the Solution Template

Deploy the 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 management center virtual in the Microsoft Azure environment. For detailed steps for Azure setup, see Getting Started with Azure.

When you deploy the 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.

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 "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 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 management center virtual administrator access. Do not use this username to log in to the 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 management center virtual.

f) Enter an **Admin Password**.

This is the password you'll use when you log in to the management center virtual's Web interface as the administrator to configure the management center virtual.

g) Choose your **Subscription** type.

Normally there is only one option listed.

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

The 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 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 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 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 management center virtual. Without a public IP address, any communication to the 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 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**.

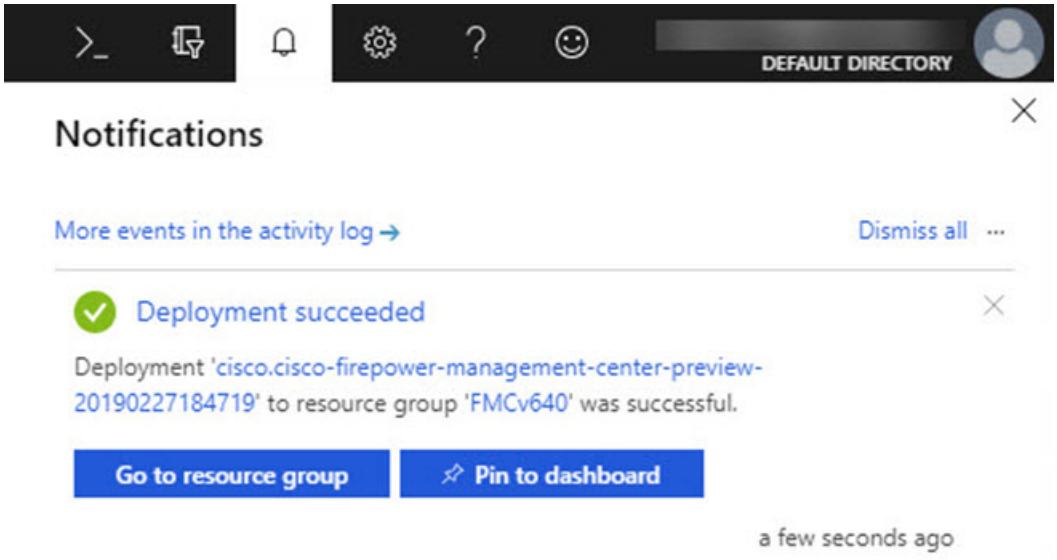
h) Click **OK**.

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 management center virtual is usable is approximately 30 minutes. Deployment times vary in Azure. Wait until Azure reports that the 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 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 management center virtual's Web interface is confirmed if you see the login prompt on either boot diagnostics or serial console.

Example:

```
Cisco Firepower Management Center for Azure v6.4.0 (build 44)
FMCv64East login:
```

What to do next

- 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 Resource Template

You can create your own custom 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 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 Management Center Virtual.

Step 1 Download the 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 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 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 **Gen 1**.

  Note **Gen 2** is not supported.

- **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 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 Management Center Virtual instances using the managed image and a resource template:

a) Select **New**, and search for **Template Deployment** until you can select it from the options.
b) Select **Create**.
c) Select **Build your own template in the editor**.

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

d) Paste your customized JSON template code into the window, and then click **Save**.
e) Choose a **Subscription** from the drop-down list.
f) Choose an existing **Resource group** or create a new one.
g) Choose a **Location** from the drop-down list.
h) Paste the Managed Image **Resource ID** from the previous step into the **Vm Managed Image Id** field.

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 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 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 Management Center Virtual's IP configuration in Azure.

Deploy the IPv6 Supported Secure Firewall Management Center Virtual on Azure

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

About IPv6 Supported Deployment on Azure

Management Center Virtual offerings support both IPV4 and IPv6 from 7.3 and later. In Azure, you can deploy 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 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 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 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 management center virtual. To use this template, see Deploy from Azure Using Custom IPv6 Template with Marketplace Image Reference, on page 13.

  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 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 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 management center virtual. See, Deploy from Azure Using a VHD and Custom IPv6 Template, on page 18.

The process involved in deploying 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 management center virtual is as follows:

Table 3:

Step	Process
1	Create a Linux VM in Azure where you are planning to deploy the IPv6-supported management center virtual
2	Enable Programmatic deployment option on Azure portal or Azure CLI **only** when you are deploying 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 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 Custom IPv6 Template with Marketplace Image Reference

The process involved in deploying management center virtual using custom IPv6 template (ARM template) in reference to marketplace image.

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 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.
b) Run the following CLI command to enable programmatic deployment for deploying custom IPv6 (ARM) template.

   During the command execution, you must only accept the terms once per subscription of the image.

   # Accept terms

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

   # Review that 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 management center virtual with BYOL subscription plan.

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

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 management center virtual.

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

Step 4 Select one of the management center virtual version from the list of available marketplace image versions that are displayed.

For IPv6 support deployment of management center virtual, you must select the 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 management center virtual custom deployment:

Parameter Name	Examples of allowed Values/Type	Description
vmName	cisco-fmcv	Name the 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 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).
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)

Parameter Name	Examples of allowed Values/Type	Description
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 management center virtual. By default it has the following three key-value pairs to configure: • 'admin' user password • management center virtual hostname • the management center virtual hostname or CSF-DM for management. 'ManageLocally : yes' - This configures the CSF-DM to be used as threat defense virtual manager. You can configure the management center virtual as threat defense virtual manager and also give the inputs for fields required to configure the same on 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'.
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.

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

Step 7 Use the ARM template to deploy 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 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 management center virtual images using a compressed VHD image available from Cisco. This process is similar to deploying 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 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 management center virtual.

Step 1 Download the 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.

   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 management center virtual parameter file. See the sample for the Azure 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 management center virtual deployment:

Parameter Name	Examples of allowed values/types	Description
vmName	cisco-fmcv	Name the 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 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.

Parameter Name	Examples of allowed values/types	Description
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 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 threat defense virtual manager. You can configure the CSF-MCv as 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, 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

Parameter Name	Examples of allowed values/types	Description
		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 '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'.

Parameter Name	Examples of allowed values/types	Description
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 management center virtual VM. Standard_D4_v2 is the default.

Step 4 Use the ARM template to deploy 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 Management Center Virtual Deployment

After the management center virtual VM is created, the Microsoft Azure Dashboard lists the new 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 management center virtual.

Before you begin

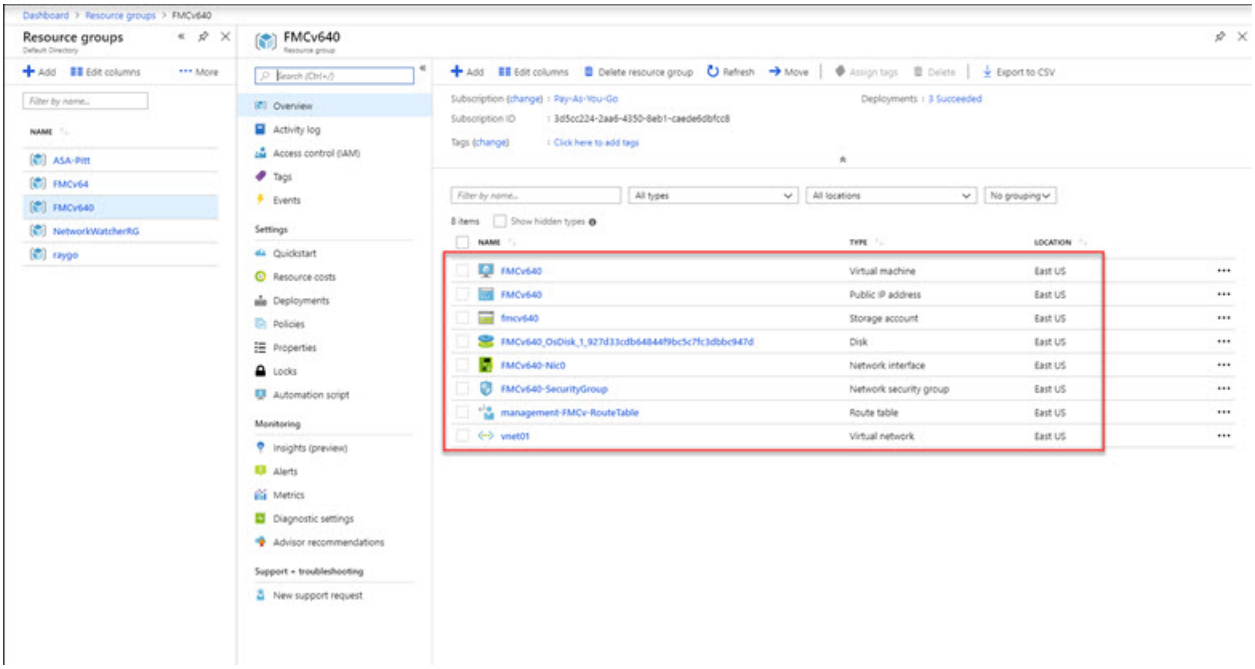
The management center virtual VM is started automatically. During deployment the status is listed as "Creating" while Azure creates the VM, and then the status changes to "Running" once the deployment is complete.

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

Step 1 To view the 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 management center virtual VM as well as its corresponding resources (storage account, network resources, etc.).

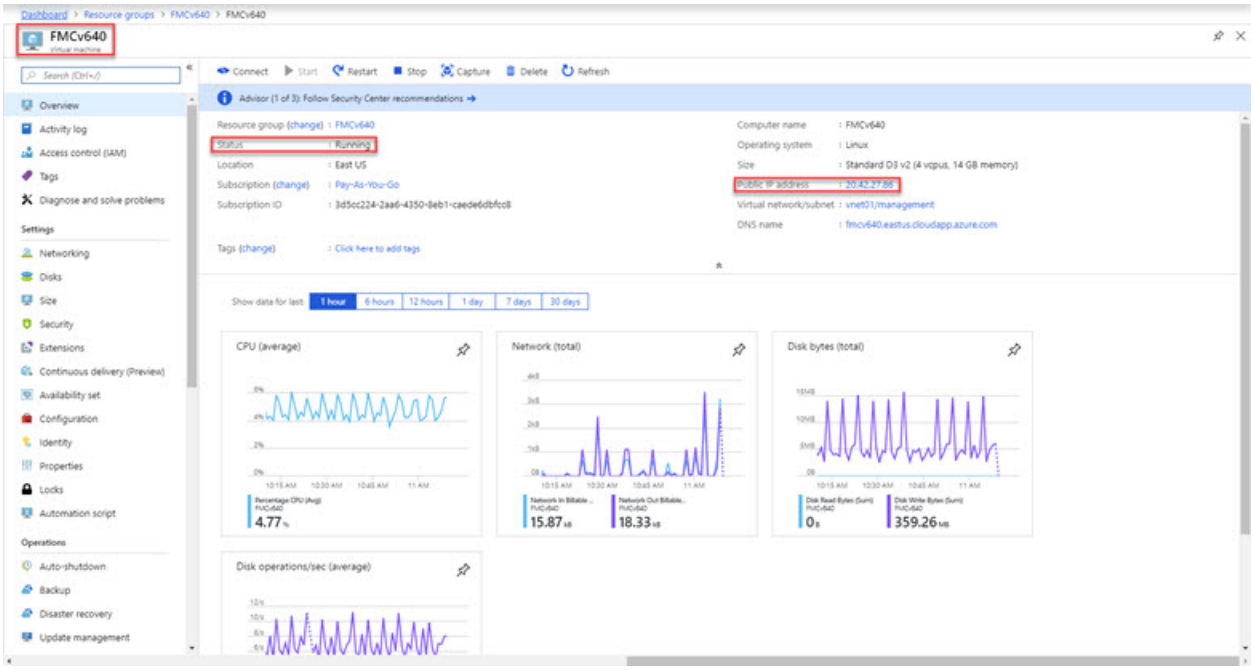
Figure 2: Azure Management Center Virtual Resource Group Page



Step 2 To view details of the management center virtual VM associated with the resource group, click the name of the management center virtual VM.

The following figure shows an example of the **Virtual machine** overview page associated with the 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 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 management center virtual; see Guidelines and Limitations, on page 3 for graceful shutdown information.

Step 3 From the **Virtual machine** page, find the **Public IP address** assigned to the 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 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 Management Center Virtual Initial Administration and Configuration 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 management center virtual appliance deployed in Micosoft Azure. Monitoring and troubleshooting can relate to either the deployment of the VM in Azure, or the 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 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 management center virtual's command line interface using the public IP address assigned to the management center virtual.

Management Center Virtual Monitoring and Logging

Troubleshoots and general logging operatations follow the same procedures as current management center and 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 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 management center has trouble provisioning for any reason, the 20 minute timer tends to end in the middle of the management center database initialization, likely resulting in a deployment failure.
- If the 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	Management Center Virtual High Availability (HA) is on the following models: FMCv10, FMCv25, and F
FMCv300 support	7.4.2	FMCv300 is supported.
Deploy the management center virtual on the Microsoft Azure public cloud.	6.4.0	Initial support.