Deploy the Firepower Management Center Virtual On the Microsoft Azure Cloud

You can deploy the Firepower Management Center Virtual (FMCv) as a virtual machine on the Microsoft Azure public cloud.

Important The FMCv is supported on Microsoft Azure starting with Cisco Firepower software version 6.4 and later.

About FMCv Deployment and Azure

You deploy the Firepower Management Center Virtual (FMCv) in Microsoft Azure using a solution template available in the Azure Marketplace. When you deploy the FMCv 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 FMCv, allowing you to login to the FMCv web interface after first boot.

FMCv Requires 28 GB RAM for Upgrade (6.6.0+)

The FMCv platform has introduced a new memory check during upgrade. FMCv upgrades to Version 6.6.0+ will fail if you allocate less than 28 GB RAM to the virtual appliance.

Important As of the Version 6.6.0 release, lower-memory instance types for cloud-based FMCv deployments (AWS, Azure) are fully deprecated. You cannot create new FMCv instances using them, even for earlier Firepower versions. You can continue running existing instances. See Table 1: Azure Supported Instances for FMCv, on page 2.

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

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

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

Table 1: Azure Supported Instances for FMCv

Platform	Version 6.6.0+	Version 6.5.x and earlier*
FMCv	Standard_D4_v2: 8 vCPUs, 28 GB	Standard_D3_v2: 4 vCPUs, 14 GB
	—	Standard_D4_v2: 8 vCPUs, 28 GB
	*Note that FMCv 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 FMCv (any version) using an instance with at least 28 GB RAM. See Resizing Instances, on page 2.	

Deprecated Instances

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

Resizing Instances

Because the upgrade path from any earlier version of FMCv (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 FMCv, 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 and System Requirements

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

Verify the following before you deploy the FMCv in Azure:

- Create an account on Azure.com.

  After you create an account on Microsoft Azure, you can log in, search the marketplace for Cisco Firepower Management Center Virtual, and choose the “Cisco Firepower Management Center (FMCv) 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
- Public IP addressing
  - The Management 0/0 is assigned a public IP address.

Licensing

The FMCv in the Azure public marketplace supports the Bring Your Own License (BYOL) model. For the FMCv, 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 Firepower 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 Firepower System* in the Firepower Management Center Configuration Guide for more information about how to manage licenses; see Cisco Firepower System Feature Licenses for an overview of feature licenses for the Firepower 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 FMCv VM. These are not graceful shutdown mechanisms and can lead to database corruption.

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

Use the `shutdown` and `restart` commands from the FMCv's command line interface to shut down or restart the appliance.

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 FMCv VM.
- High Availability (active/standby)
- VM import/export

Resources Created During Deployment

When you deploy the FMCv in Azure the following resources are created:

- A Cisco FMCv Virtual Machine (VM) with a single interface (requires a new or an existing virtual network with 1 subnet).
- A Resource Group.

  The FMCv 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 Firepower 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 FMCv 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 Firepower Management Center Virtual

You can deploy the Firepower 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 FMCv 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 5.
- **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 FMCv 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 FMCv in a single, coordinated operation.

Deploy from Azure Marketplace Using the Solution Template

Deploy the Firepower Management Center Virtual (FMCv) 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 FMCv in the Microsoft Azure environment. For detailed steps for Azure setup, see Getting Started with Azure.

When you deploy the FMCv 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 “Cisco Firepower Management Center (FMCv)”, choose the offering, and click **Create**.

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 FMCv administrator access. Do not use this username to log in to the FMCv.

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 FMCv.

f) Enter an **Admin Password**.

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

g) Choose your **Subscription** type.

Normally there is only one option listed.

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

The FMCv 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 FMCv 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 FMCv, 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 FMCv 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 FMCv. Without a public IP address, any communication to the FMCv 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 FMCv.

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

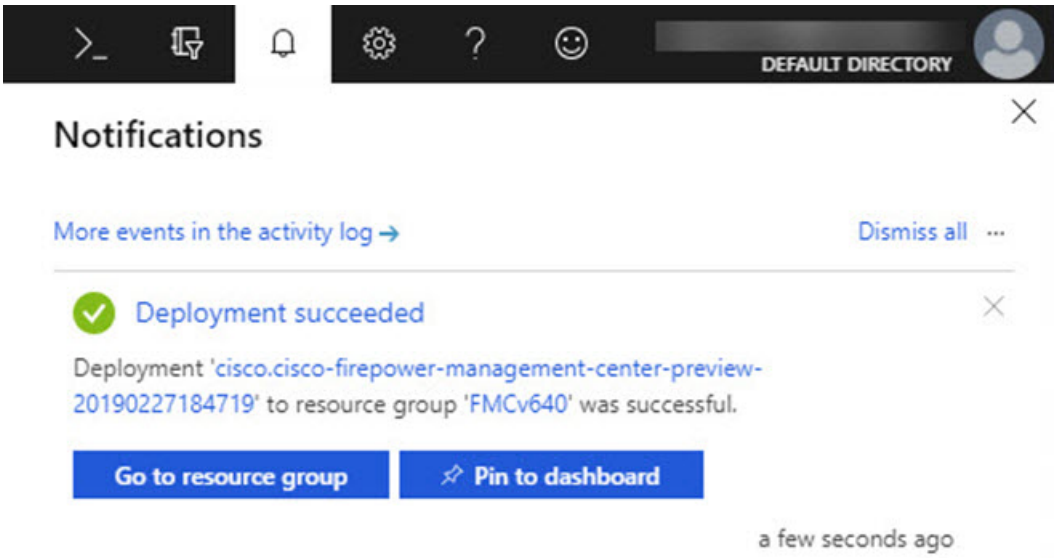
g) Click **OK**.

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 FMCv is usable is approximately 30 minutes. Deployment times vary in Azure. Wait until Azure reports that the FMCv 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 FMCv 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 FMCv'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 FMCv deployment was successful. The Azure Dashboard lists the new FMCv VM under Resource Groups, along with all of the related resources (storage, network, route table, etc.).

Verify the Firepower Management Center Virtual Deployment

After the FMCv VM is created, the Microsoft Azure Dashboard lists the new FMCv 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 FMCv.

Before you begin

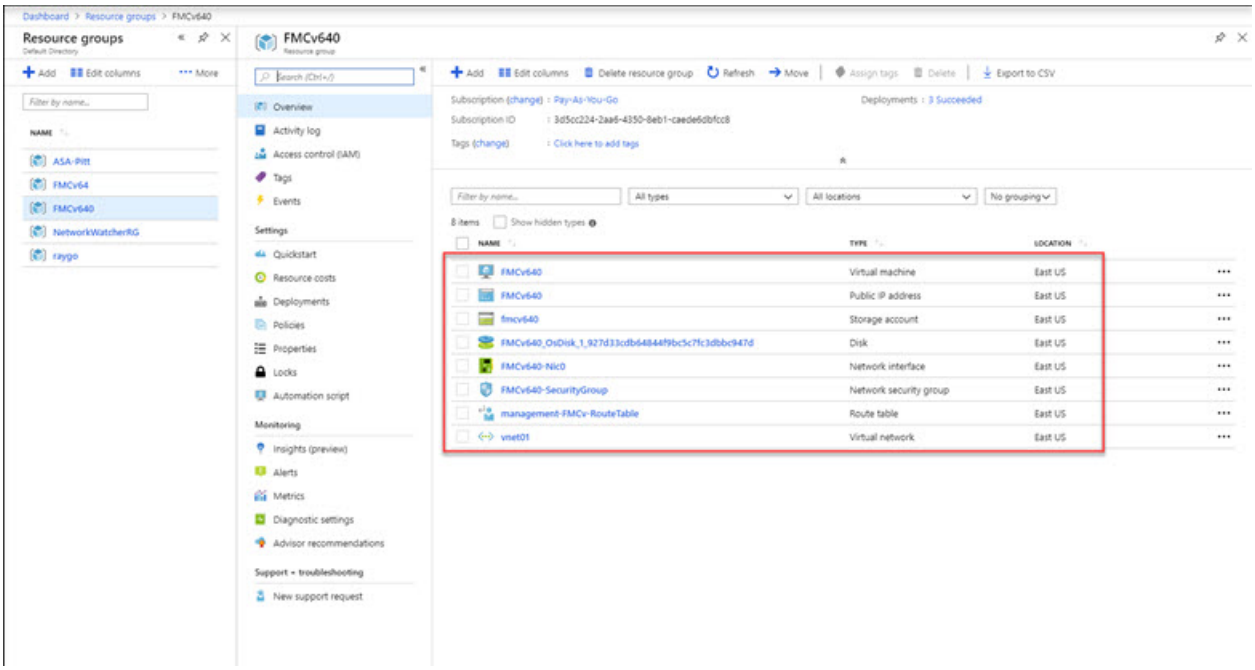
The FMCv VM is started automatically. During deployment the status is listed as "Creating" while Azure creates the VM, and then the status changes to "Running" once the deployment is complete.

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

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

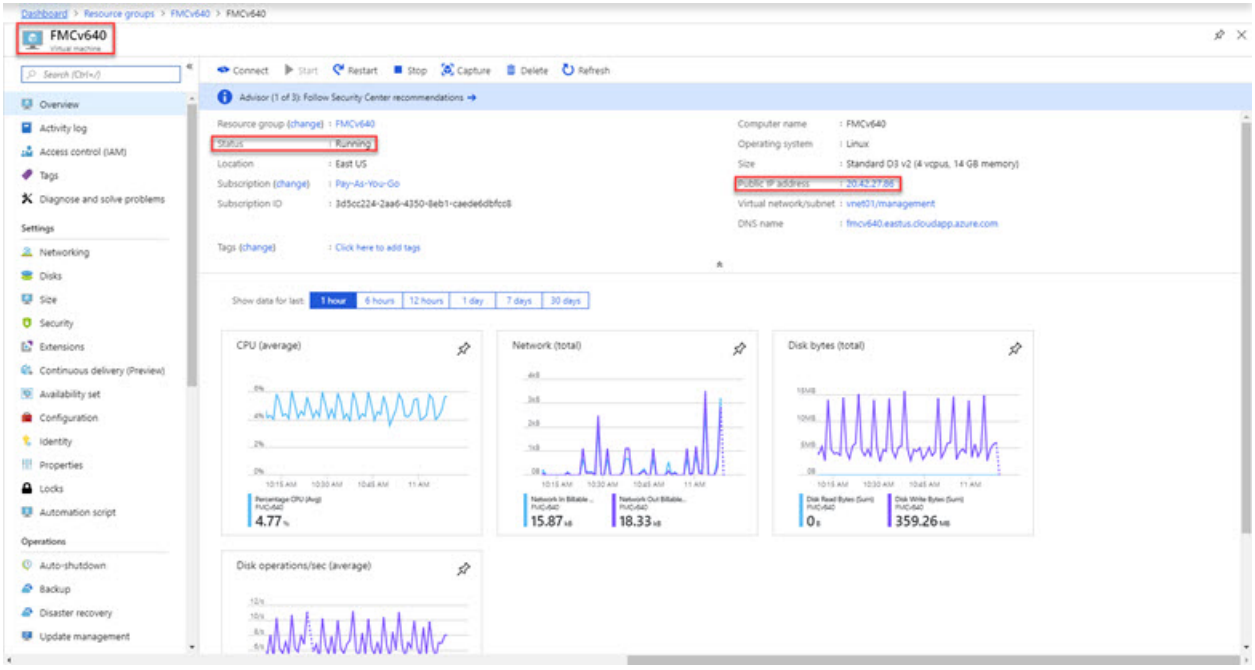
Figure 2: Azure FMCv Resource Group Page



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

The following figure shows an example of the **Virtual machine** overview page associated with the FMCv 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 an FMCv VM from the **Virtual machine** page in the Microsoft Azure portal. Note that these controls are not graceful shutdown mechanisms for the FMCv; 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 FMCv.

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 theFMCv'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 Firepower 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 Firepower system, see the complete Firepower Management Center Configuration Guide for your software version.

Monitoring and Troubleshooting

This section includes general monitoring and troubleshooting guidelines for the Firepower Management Center Virtual appliance deployed in Micosoft Azure. Monitoring and troubleshooting can relate to either the deployment of the VM in Azure, or the FMCv 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 FMCv 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 FMCv's command line interface using the public IP address assigned to the FMCv.

FMCv Monitoring and Logging

Troubleshoots and general logging operatations follow the same procedures as current FMC and FMCv models. Refer to the *System Monitoring and Troubleshooting* section of the Firepower 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 FMC 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 FMC has trouble provisioning for any reason, the 20 minute timer tends to end in the middle of the FMC database initialization, likely resulting in a deployment failure.
- If the FMC 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.

History for FMCv On the Microsoft Azure Cloud

Feature Name	Releases	Feature Information
Deploy the Firepower Management Center Virtual (FMCv) on the Microsoft Azure public cloud.	6.4.0	Initial support.