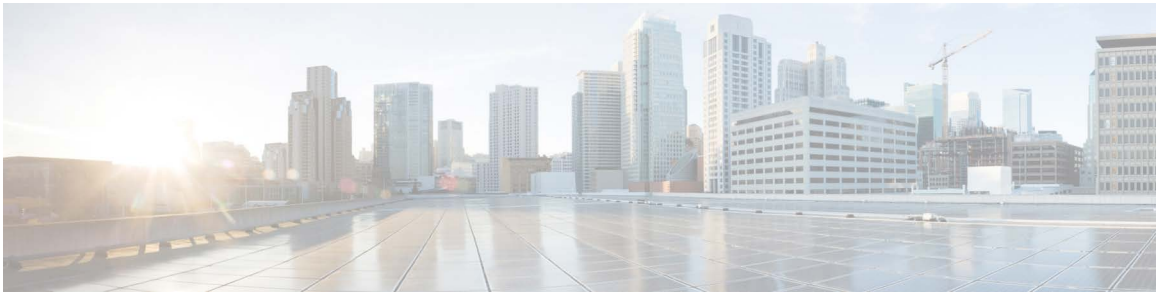


# Deploying Cisco Secure Email Virtual Gateway and Cisco Secure Email and Web Manager Virtual on Microsoft Azure Cloud Platform

**Published: May 4, 2023**

## Contents



## Prerequisites

Before you begin the deployment activity, make sure you have the following details available:

- Microsoft Azure account credentials
- Any web browser to launch the Azure portal (https://portal.azure.com/)
- Secure Email Virtual Gateway or Secure Email and Web Manager Virtual Image
- License (Classic or Smart License)
- [Optional] CentOS or Windows system with Azure CLI or PowerShell installed

**Cisco Systems, Inc.**
www.cisco.com

# Suggested Azure VM Size

| Virtual Model | Azure VM Size | vCPU/cores | Memory (RAM) | NICs |
|---|---|---|---|---|
| C600V | Standard D8s v3 | 8 | 32 | 4* |
| M600V | Standard D8s v3 | 8 | 32 | 4* |

**Note** *Secure Email Virtual Gateway and Secure Email and Web Manager Virtual support a maximum of **three** interfaces.

**Note** The Azure virtual machine OS disk size for Secure Email and Web Manager Virtual M600v model is reduced from 2 TB to 1 TB due to the limitation of sharing images with the OS disk greater than 1024 GB in the Azure compute gallery.

# How to Create Secure Email Gateway or Secure Email and Web Manager Instance on Azure Platform

Perform these steps in order:

| Steps | Do This | More Information |
|---|---|---|
| 1 | Create the required components. | Creating Components, page 2 |
| 2 | Obtain the VM image. | Getting Secure Email Virtual Gateway or Secure Email and Web Manager Virtual Image, page 7 |
| 3 | Configure Access Control - Identity and Access Management (IAM). | Configuring Access Control (IAM), page 8 |
| 4 | Log in and create the VM. | Logging in and Creating Virtual Machine, page 10 |

# Creating Components

**Before You Begin**:
Make sure you are able to access the Azure CLI. For more information, see Accessing the CLI, page 2.

## Accessing the CLI

If Azure CLI is not installed in the client system, log in to the Microsoft Azure portal. You can use the **cloud shell** option next to the global search tool.

***Figure 1 Global Search Tool***

**Note**

- Do not use a line break (newline character) for any command if you copy and use the same content. Line breaks are used for readability purpose only. Replace the line break with a single space. For example,

```
az group create
    --name cisco-rg
    --location eastus
```

  You must execute this command as: `az group create --name cisco-rg --location eastus`

- The ’ symbol, wherever used for some commands, is the single quote (') and not the backquote (`).
- An extra line break or blank space could be introduced when you copy a lengthy URL or path. You must remove this extra space when you copy the text to the CLI or browser; otherwise, you may see an 'invalid argument' error.

**Procedure**:

You can use the following steps in sequence to create the components:

1. Creating Resource Group

2. Creating Storage Account

3. Creating Network Security Group

4. Setting Rules in Network Security Group

5. Creating Virtual Network and Subnets

6. Creating Single Network Interface

7. Creating Multiple Network Interfaces

**Note** The commands mentioned in the examples in the following procedure steps (**1** to **7**) are used to create one secure email gateway instance.

**Note** The Secret Values and Azure Image path are valid for a specific period of time. Contact Cisco TAC if Secret Values and Azure Image path are expired. The Secret Value and Azure Image path details are sent to you by email.

# 1. Creating Resource Group

Execute the following command in the CLI:

```
az group create
     --name <resource group name>
    --location <location  name>
```

**Example**:

```
az group create
    --name cisco-rg
    --location eastus
```

# 2. Creating Storage Account

Execute the following command in the CLI:

```
az storage account create
    --resource-group <resource group name>
    --name <storage account name>
    --location <location id>
    --sku Standard_LRS
    --kind StorageV2
```

**Example**:

```
az storage account create
    --resource-group cisco-rg
    --name ciscosa
    --location eastus
    --sku Standard_LRS
    --kind StorageV2
```

# 3. Creating Network Security Group

**Note** See the "Firewall Information" chapter in the appropriate user guide to view the list of ports to be opened for the proper operation of Secure Email Gateway or Secure Email and Web Manager Virtual.

Execute the following command in the CLI:

```
az network nsg create
    --resource-group <resource group name>
    --name <security group name>
```

**Example**:

```
az network nsg create
    --resource-group cisco-rg
    --name cisco-nsg
```

# 4. Setting Rules in Network Security Group

Execute the following command in the CLI:

```
az network nsg rule create
    --resource-group <resource group name>
    --nsg-name <security group name>
    --name <Rule Name>
    --access <Allow/Deny>
    --protocol <protocol type>
    --direction <Inbound/Outbound>
    --priority <Rule ID>
    --source-address-prefix <source subnet range>
```

```
    --source-port-range <port range>
    --destination-port-range <port range>
    --description  <description  or  comments>
```

**Example**:

```
az network nsg rule create
    --resource-group cisco-rg
    --nsg-name cisco-nsg
    --name  All_Port_Traffic
    --access Allow
    --protocol  "*"
    --direction Inbound
    --priority  110
    --source-address-prefix "*"
    --source-port-range "*"
    --destination-port-range  "*"
    --description "Opening traffic on all ports"
```

# 5. Creating Virtual Network and Subnets

Execute the following command in the CLI:

```
az network vnet create
    -g <resource group name>
    -n <virtual network name>
    --address-prefix <address space>
    --network-security-group <security group name>
az network vnet subnet create
    -g <resource group name>
    -n <virtual network name>
    --address-prefix <address space>
    --subnet-name <subnet name>
    --subnet-prefix <subnet with netmask>
    --network-security-group <security group name>
```

**Example**:

```
az network vnet create
    -g  cisco-rg
    -n cisco-vnet
    --address-prefix  10.1.0.0/16
    --network-security-group cisco-nsg
az network vnet subnet create
    -g  cisco-rg
    --vnet-name cisco-vnet
    -n cisco-mgmt-subnet
    --address-prefixes  10.1.0.0/24
    --network-security-group cisco-nsg
az network vnet subnet create
```

```
    -g  cisco-rg
    --vnet-name cisco-vnet
    -n  cisco-data1-subnet
    --address-prefixes  10.1.1.0/24
    --network-security-group cisco-nsg
az network vnet subnet create
    -g  cisco-rg
    --vnet-name cisco-vnet
    -n  cisco-data2-subnet
    --address-prefixes  10.1.2.0/24
    --network-security-group  cisco-nsg
```

# 6. Creating Single Network Interface

**Note** You can either create a single network interface (NIC) or multiple NICs (as described in step 7. Creating Multiple Network Interfaces) based on your requirements.

Execute the following command in the CLI:

```
az network nic create
    --resource-group <resource group name>
    --name <network interface name>
    --vnet-name <virtual network name>
    --subnet <subnet name>
    --network-security-group <security group name>
```

**Example**:

```
az network nic create
    --resource-group cisco-rg
    --name cisco-mgmt-nic
    --vnet-name cisco-vnet
    --subnet cisco-mgmt-subnet
    --network-security-group  cisco-nsg
```

# 7. Creating Multiple Network Interfaces

You can execute the same command used to create a single network interface with different interface names for multiple NICs.

**Example**:

In the following example, three NICs are created - one NIC is mapped to the management interface, and the other two NICs are mapped to data interfaces.

```
az network nic create
    --resource-group cisco-rg
    --name cisco-mgmt-nic
    --vnet-name cisco-vnet
```

```
    --subnet cisco-mgmt-subnet
    --network-security-group cisco-nsg
az network nic create
    --resource-group cisco-rg
    --name  cisco-data1-nic
    --vnet-name cisco-vnet
    --subnet  cisco-data1-subnet
    --network-security-group cisco-nsg
az network nic create
    --resource-group cisco-rg
    --name  cisco-data2-nic
    --vnet-name cisco-vnet
    --subnet  cisco-data2-subnet
    --network-security-group  cisco-nsg
```

# Getting Secure Email Virtual Gateway or Secure Email and Web Manager Virtual Image

**Note** An extra line break or blank space could be introduced when you copy a lengthy URL or path. You must remove this extra space when you copy the text to the CLI or browser; otherwise, you may see an 'invalid argument' error.

**Procedure**:

**Step 1** Open the preferred web browser and go to the following URL.

**Step 2** Example of URL format:
`https://login.microsoftonline.com/<TenantID>/oauth2/authorize?client_id=<ApplicationID>&response_type=code&redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F`

**Note** You can use the following URL format for Azure deployment in the China region:
`https://login.chinacloudapi.cn/<Tenant 2 ID>/oauth2/authorize?client_id=<Application (client) ID>&response_type=code&redirect_uri=https%3A%2F%2Fwww.microsoft.com%2F`

**Step 3** Log in using your Azure account credentials.

**Step 4** Replace `<TenantID>` with your Azure Tenant ID to obtain access to the image in the resource groups in the URL mentioned in step 1.

**Note** You can get th*e* **<**`TenantID>` from the Azure Active Directory resource.

**Note** The <ApplicationID> (also known as the *Client ID*) is provided by Cisco.
You can use the Cisco <ApplicationID> -3243d803-7fc5-4329-829e-e08c5614c4d2 in the URL mentioned in step 1.
Contact Cisco Technical Assistance if you need support.

After you replace the <TenantID> and <ApplicationID>, the URL looks like:

```
https://login.microsoftonline.com/8e1c37c0-b056-432e-81a7-44b1110c95c1/oauth2/authorize
?client_id=3243d803-7fc5-4329-829e-e08c5614c4d2&response_type=code&redirect_uri=https%3
A%2F%2Fwww.microsoft.com%2F
```

# Configuring Access Control (IAM)

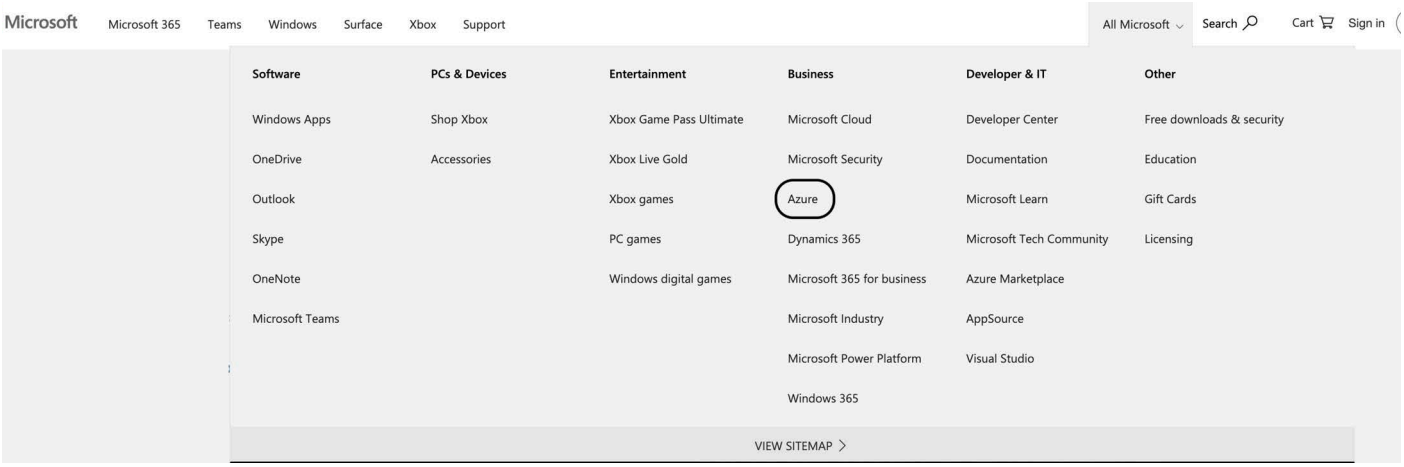
**Procedure**:

**Step 1** Log in with your Azure account credentials when you access the URL mentioned in step1 of Getting Secure Email Virtual Gateway or Secure Email and Web Manager Virtual Image, page 7.

The page redirects to the Microsoft (microsoft.com) home page.

**Step 2** Select **Azure** listed under "All Microsoft" drop-down list in the top-right corner of the page.

***Figure 2 Microsoft Home page***



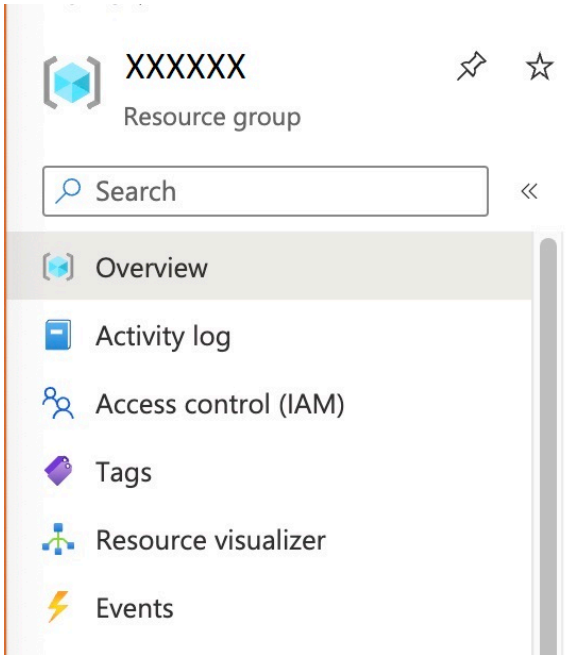

**Step 3** Click on the **Sign In** option on the top right-side of the page.

You are logged into your Azure account and can view the Azure Dashboard.

**Step 4** Select the **Resource Group** to which you need to add the shared image.

**Step 5** Select **Access Control (IAM)** in the Resource Group,

*Figure 3 Resource Group*




**Step 6** Select **Add role assignment** under "Grant access to this resource" in the IAM window.

A new window opens.

**Step 7** Select **Contributor** under Role and click **Next**.

**Step 8** Select **User**, **Group** or **Service Principal** to assign access.

**Step 9** Click the **Select Members** link.

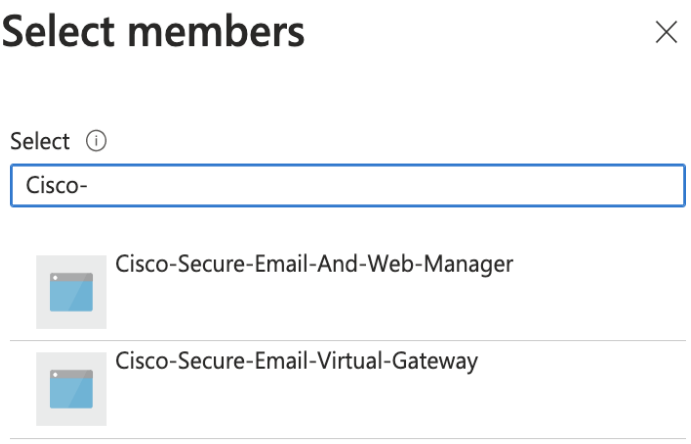
**Step 10** [Applicable for Secure Email Gateway users]: Search for **ESA — Cisco-Secure-Email-Virtual-Gateway** in the "Select Members" window.

OR

[Applicable for Secure Email and Web Manager users]: Search for **SMA — Cisco-Secure-Email-And-Web-Manager** in the "Select Members" window.

**Step 11** Select the required Secure Email Virtual Gateway or Secure Email and Web Manager version from the search result.

*Figure 4 Select Members window*




After you select the member (for example, “ESA — Cisco-Secure-Email-Virtual-Gateway” as shown in the figure in step 11), it appears under members list, with type category as “App.”

**Step 12** Click **Next** and then click **Review + Assign**.

**Note** You need to use either Azure CLI, PowerShell, or CloudShell to create a VM from the image shared through Azure Compute Gallery.

# Logging in and Creating Virtual Machine

Perform these steps in order:

**Step 1** Log in to the cloudshell CLI.

If Azure CLI is not installed in the client system, log in to the Microsoft Azure portal. You can use the **cloud shell** option next to the global search tool.

*Figure 5 Global Search tool*


**Note**

- Do not use a line break (newline character) for any command if you copy and use the same content. Line breaks are used for readability purpose only. Replace the line break with a single space.
- The ’ symbol, wherever used for some commands, is the single quote (') and not the backquote (`).
- An extra line break or blank space could be introduced when you copy a lengthy URL or path. You must remove this extra space when you copy the text to the CLI or browser; otherwise, you may see an 'invalid argument' error.

**Step 2** Run the following command in the cloud shell.

```
az login
    --service-principal
    -u '<Application ID>'
    -p '<Secret Value>'
    --tenant '<Cisco Tenant ID>'
```

**Note** The `<Application ID>`, `<Secret Value>`, and `<Tenant ID>` are shared by Cisco. In the command mentioned in step 2, the `<Tenant ID>` used is Cisco's Tenant ID. Contact Cisco TAC if you need support.

**Example**:

```
az login
      --service-principal
      -u '3243d803-7fc5-4329-829e-e08c5614c4d2'
      -p 'qRG8Q~98CjkILX3deMT3X4DGz7rr36uTpIUrOaNv'
      --tenant '18965413-d29e-40cb-a6e7-79aa456932b7'
```

You get the following response:

```
[
  {
    "cloudName": "AzureCloud",
    "homeTenantId": "18965413-d29e-40cb-a6e7-79aa456932b7",
    "id": "c9554b3f-247f-46b8-b0df-453c91e115ae",
    "isDefault": true,
    "managedByTenants": [],
    "name": "Primary Cisco Account",
    "state": "Enabled",
    "tenantId": "18965413-d29e-40cb-a6e7-79aa456932b7",
    "user": {
      "name": "3243d803-7fc5-4329-829e-e08c5614c4d2",
      "type": "servicePrincipal"
    }
  }
]
```

**Step 3** Run the `az account get-access-token` command in the cloud shell.

You get the following response:

```
{
  "accessToken": "eyJ0eXAiOiJKV1QiLCJhbqKZi9W8MRfCtw",
  "expiresOn": "2022-08-29 20:23:43.000000",
  "subscription": "c9554b3f-247f-46b8-b0df-453c91e115ae",
  "tenant": "18965413-d29e-40cb-a6e7-79aa456932b7",
  "tokenType": "Bearer"
}
```

**Note** The access token has a validity period.

**Step 4** Run the **az login** command again with your Tenant ID instead of the Cisco Tenant ID.

```
az login
    --service-principal
    -u '<Application ID>'
    -p '<Secret Value>'
    --tenant '<Client Tenant ID>'
```

**Example**:

```
az login
      --service-principal
      -u '3243d803-7fc5-4329-829e-e08c5614c4d2'
      -p 'qRG8Q~98CjkILX3deMT3X4DGz7rr36uTpIUrOaNv'
      --tenant '972e674c-3473-4c04-b501-0825a01c25a2'
```

**Note** In step 4, the `<Tenant ID>` used is your Tenant ID.

You get a similar response as mentioned in step 2.

**Step 5** Run the `az account get-access-token` command in the cloud shell.

You get a similar response as metioned in step 3.

**Step 6** Run the `az vm create` command in the Creating Virtual Machines, page 12 to create a virtual machine.

# Creating Virtual Machines

You must execute the `az vm create` command before the validity of the access tokens (generated in step 3 of Logging in and Creating Virtual Machine, page 10) expire. Use the same user name and password provided in the following example.

**Note** Do not replace the user name and password with any other credentials.

```
az vm create
    --resource-group <resourcegroup in which the vm needs to be created>
    --name <vm name>
    --image <this is shared image gallery path that will be shared by cisco>
    --size <VM size>
    --admin-username <username 'admin' cannot be used, so enter a dummy username>
    --admin-password <similarly enter a dummy password>
    --nics <network interfaces using which VM comes up>
    --public-ip-sku Standard
```

**Example**:

```
az vm create
    --resource-group cisco-rg
    --name cisco-01
    --image
```

```
'/subscriptions/c9554b3f-247f-46b8-b0df-453c91e115ae/resourceGroups/cisco-cs-rg/pro
viders/Microsoft.Compute/galleries/CiscoContentSecurity/images/14.0.2/versions/14.0
.2'
--size Standard_D8s_v3
--admin-username dummy
--admin-password Dummy@123456
--nics cisco-mgmt-nic cisco-data1-nic cisco-data2-nic
--public-ip-sku Standard
```

After you run this command in the cloud shell, it moves to the "running" state. You must ensure that a new instance is created in virtual machines with the VM name provided. The virtual machine remains in the “running” state itself.

If you see a 'Microsoft.Network' or 'Microsoft.Compute' error message such as *“Resource provider 'Microsoft.Network' used by this operation is not registered. We are registering for you. Registration failed. Please register manually,"* you must register the Resource Provider for your subscription from the Azure portal manually. Contact Cisco TAC for further assistance.

**Note**

- Even though the virtual instance is created successfully, an error message may appear after the VM creation command is executed and the deployment status from Azure could be marked as “Failed” or “Timed Out.” You can ignore this message. This issue will be addressed in upcoming builds.
- You can use boot diagnostics or serial console to know the actual state of the VM created.
- The command executed in the cloud shell to create virtual machines does not stop automatically. You need to cancel the command manually by pressing “Ctrl + C" once VM comes up successfully.
- Default username and password (admin or ironport) are used to connect to the VM. Dummy username and password are not used.
- The Generation 2 Image does not boot after you deploy it on the Azure platform. You must reboot the virtual machine after you deploy the Generation 2 image.

# Known Issues

The following list of known issues are applicable to AsyncOS 15.0 - Secure Email Virtual Gateway and Secure Email and Web Manager Virtual:

- CSCwe45170: [AZURE] 15.0 Gen2 image unable to boot up with D8s_v3 instance size & Standard HDD
- CSCwd70737 - Azure: [ESA/SMA] - Azure instances fail to boot intermittently
- CSCwa52321: [azure] Disk size is shown as '0' for ipcheck command output.
- CSCwa52346: [azure] Platform is shown as 'unknown' for ipcheck command output.
- CSCwa52452: [azure] gpart show command prints the da1 partition, which is not expected.
- CSCwa68102: Spam quarantine page is not loading in NAT environment even when the hostname is configured for Spam quarantine in the Interface page.

## Getting Support for Virtual Gateways

**Note** To get support for virtual gateways, call Cisco TAC and have your Virtual License Number (VLN) number ready.

If you file a support case for Cisco Secure Email Virtual Gateway or Cisco Secure Email and Web Manager Virtual, you must provide your contract number and your Product Identifier code (PID).

You can identify your PID based on the software licenses running on your virtual gateway, by referencing your purchase order.

# Related Documentation

For more information, including information about support options, see the Release Notes and User Guide or online help for your AsyncOS release.

| Documentation for Cisco Secure Email Product: | Location |
|---|---|
| Cisco Secure Email Virtual Gateway | https://www.cisco.com/c/en/us/support/security/email-security-virtual-appliance/series.html |
| Cisco Secure Email and Web Manager Virtual | https://www.cisco.com/c/en/us/support/security/content-security-management-virtual-appliance/series.html |

# Service and Support

**Note** To get support for virtual appliances, call Cisco TAC and have your Virtual License Number (VLN) number ready.

Cisco TAC: http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

Support site for legacy IronPort: Visit http://www.cisco.com/web/services/acquisitions/ironport.html

For non-critical issues, you can also access customer support from the appliance. For instructions, see the User Guide or online help.