

# FORTRA

Clearswift Secure Email Gateway  
Version 5.7.0

**Installation Guide**  
(on Microsoft Azure)

## Copyright Terms and Conditions

---

Copyright © Fortra, LLC and its group of companies. All trademarks and registered trademarks are the property of their respective owners.

The content in this document is protected by the Copyright Laws of the United States of America and other countries worldwide. The unauthorized use and/or duplication of this material without express and written permission from Fortra is strictly prohibited. Excerpts and links may be used, provided that full and clear credit is given to Fortra with appropriate and specific direction to the original content.

202403270622

# Contents

---

<b>Copyright Terms and Conditions</b> .....	<b>ii</b>
<b>Contents</b> .....	<b>iii</b>
<b>1. About this guide</b> .....	<b>5</b>
1.1 Who is this guide for? .....	5
<b>2. Before installing</b> .....	<b>6</b>
2.1 Types of installation .....	6
2.2 Prerequisites .....	6
Browser support .....	6
<b>3. Configure a virtual machine using Microsoft Azure</b> .....	<b>7</b>
3.1 Create the VM .....	7
3.2 Configure the basic settings .....	7
Project Details .....	7
Instance details .....	7
Administrator account .....	8
Inbound port rules .....	8
3.3 Configure the disk settings .....	8
Disk options .....	9
Data disks .....	9
3.4 Configure the networking settings .....	9
Network interface .....	9
Load balancing .....	10
3.5 Configure the additional settings .....	10
3.6 Review and create the VM .....	10
Generate new key pair .....	11
3.7 Configure public IP address and DNS name .....	11
3.8 Increase the disk size .....	11
3.9 Enlarge the OS partition .....	12
<b>4. Install Clearswift Secure Email Gateway</b> .....	<b>15</b>
4.1 Install from the Clearswift online repositories .....	15
4.2 Configure your Red Hat Enterprise Linux installation .....	16
Enable online repositories .....	16
Create administrator accounts .....	17

4.3 Configure Secure Email Gateway .....	18
4.4 Configure update repositories .....	18
4.5 How to change your network settings .....	18
<b>5. Upgrade .....</b>	<b>20</b>
<b>Appendix A: Configure multiple NICs on Azure .....</b>	<b>21</b>
Log in .....	21
Collect and configure your resources .....	21
Create your VM .....	24
Required parameters .....	24
Red Hat images and sizing .....	25
Create the VM using your parameters .....	26
Check Azure displays your VM .....	27
<b>Contact Fortra .....</b>	<b>28</b>
Fortra Support Portal .....	28

# 1. About this guide

---

This guide provides information for administrators installing Clearswift Secure Email Gateway onto a virtual machine. It covers the procedures and requirements necessary for a full installation.

## 1.1 Who is this guide for?

This guide is intended for use by:

- Customers installing Clearswift Secure Email Gateway version 5.7.0 on the Microsoft Azure platform.
-

## 2. Before installing

---

This section outlines prerequisites and considerations you need to make before installing the cloud-hosted Secure Email Gateway.

The Gateway runs on 64 bit Red Hat Enterprise Linux (RHEL) 7.9.

### 2.1 Types of installation

You can install Secure Email Gateway on a virtual machine using Microsoft Azure.

Note that:

- This guide covers the installation of a new instance of Secure Email Gateway on a Microsoft Azure platform only. It does not cover installation on the Azure Classic Portal.

For alternative installation types, please refer to the [Installation & Getting Started Guide](#).

- For the **Personal Message Management (PMM)** feature, you must install a separate network interface controller.

This requires different installation steps, which are covered in [Appendix A: Configuring multiple NICs on Azure](#) of this guide.



The use of online repositories will download updates to your system. Microsoft will charge your Azure account for these transfers.

### 2.2 Prerequisites

Before installing, ensure that you have the following:

- A valid Microsoft Azure account
- Your subscription details

#### Browser support

Secure Email Gateway supports connections using TLS 1.2 ciphers and has been tested with the following browsers:

- Mozilla Firefox - latest
- Google Chrome - latest
- Microsoft Edge (Windows 10)

## 3. Configure a virtual machine using Microsoft Azure

---

The following steps show you how to create the Azure virtual machine (VM) required to host Secure Email Gateway using the Microsoft Azure Management Portal.



For detailed instructions on using external resources, such as the Microsoft Azure Management Portal, refer to the appropriate documentation by the providers. Fortra is not responsible for changes to any of the procedure steps described.

### 3.1 Create the VM

1. Sign in to the [Microsoft Azure Management Portal](#).
2. From the hub menu, click **Create a resource (+)**.
3. From the **Categories**, select **Compute**.
4. From the **Marketplace**, select a virtual machine.

### 3.2 Configure the basic settings

Use the **Basics** side menu to configure the details of your virtual machine.

#### Project Details

1. Select your **Subscription**.
2. Select your **Resource group**.

#### Instance details

1. Enter your **Virtual machine name**. This cannot be changed once the VM has been created.
2. Select the nearest data center for your **Region**. You will need this information in order to log in to the machine later.



Some regions might have limitations on available disk types and disk sizes. For more information on what is available, see <https://azure.microsoft.com/en-us/regions/>.

3. Set **Availability options** as per the current policy of your organization.
4. Under **Image**, click **See all images**. In the Marketplace, search for Red Hat. From the **Red Hat Enterprise Linux** blade, select a **Red Hat Enterprise Linux**

7.9 option.

5. Select **Run with Azure Spot discount** as per the current policy of your organization.
6. From the **Size** drop-down menu, click **See all sizes** to select the VM size. We recommend a VM with 16 GB of RAM, such as **Standard\_E2s\_v5** or similar for production use.

### Administrator account

For the **Authentication type**, select either **SSH public key** or **Password**.

If you selected **SSH public key**:

- Enter **User name**.
- Select the **SSH public key source** as **Generate new key pair**. If required, you can use an existing key that you have previously generated from the drop-down menu.
- Enter **Key pair name**.



The SSH key pair is generated and made available as a `.pem` file that can be downloaded once the VM has been created.

If you selected **Password**:

- Enter **User name** and **Password**. Ensure that your password satisfies the Microsoft's password requirements.

### Inbound port rules

Unless otherwise required by your organizational policy, the settings in this section can be left to the default. You can use the [Networking](#) tab to create access rules for known IP addresses.

Click **Next: Disks** to continue.



At this point, you can click **Review + create** to review the basic configuration and create the VM.

However, you will need to go back and configure Disks, Networking and Management options later. Our recommendation is to configure these options prior to using **Review + create**.

## 3.3 Configure the disk settings

Use the **Disks** tab to configure the disk options and data disks of your virtual machine.



## Disk options

Configure **OS disk type** and **Encryption type** to the settings recommended by your organization.



Microsoft Azure virtual machines are automatically given a default disk size of 64 GB.

## Data disks

If required, additional disks can be added or existing disks can be attached to this VM. For detailed instructions, refer to the appropriate Azure documentation.

Click **Next: Networking** to continue.

## 3.4 Configure the networking settings

Use the **Networking** tab to configure the network interface options of your virtual machine.

### Network interface

1. From the **Virtual network** drop-down menu, select an existing virtual network. Alternatively, click **Create new** to add a new one.
2. Select a virtual network as the **Subnet**. The default network location is `10.0.0.0/24`. This is used internally and is not the public IP address that you will use to access your VM. This is specified by **Public IP Address**, which enables you to customize a name for access to the machine.



This is currently a dynamic IP address and will need amending to a static IP address later in the installation.

3. For **Network Security Group**, we recommend adding an **Advanced** level with firewall rules, configured as follows:

Priority	Name	Port	Protocol	Source	Destination
1000	Allow-ssh	22	TCP	<Your IP address>	VirtualNetwork
1010	Allow-admin-ui-access	443	TCP	<Your IP address>	VirtualNetwork
1020	Allow-cockpit-access	9090	TCP	<Your IP address>	VirtualNetwork
1030	Allow-smtp-in	25	TCP	Anywhere	VirtualNetwork



To configure the Firewall ports and protocols for the product you are installing, see [Firewall ports](#) in the Online Help.

4. Unless otherwise required by your organizational policy, the **Accelerated networking** setting can be left to the default.

#### Load balancing

Unless otherwise required by your organizational policy, the **Load balancing** setting can be left to the default.

Click **Next: Management** to continue.

### 3.5 Configure the additional settings

The **Management**, **Advanced**, **Monitoring** and **Tags** tabs are available to configure further options for your virtual machine.

- **Management and Monitoring:** Use these tabs to configure management and monitoring options for your VM.
- **Advanced:** Use this tab to add additional configuration, agents, scripts or applications as well as host and capacity reservations.
- **Tags:** Use this tab to define name/value pairs that enable you to categorize resources for use in the user interface.



When you review the options on these tabs, refer to your organization's current policy and recommendations.

When ready, click **Review + create**.

### 3.6 Review and create the VM

Use the **Review and Create** tab to check that your settings are correct and validation has passed. Once satisfied with your configuration, you can create the virtual machine.

1. Scroll through the page to review the current configuration of your VM. If any settings need amending, click **Previous** until you arrive at the tab in which the setting is defined.
2. Click **Next** to return to the **Review and Create** tab.
3. Once satisfied, click **Create** to create the VM.

### Generate new key pair

If you selected to access the VM using a newly generated **SSH public key** in the [Basic settings](#) tab, you are now prompted to download the new key.

1. Click **Download private key and create resource**.
2. When prompted, save the `.pem` file to a safe location using Windows Explorer.

## 3.7 Configure public IP address and DNS name

In the **All resources** section, the details of configured virtual machines are displayed.

1. Click your **VM name** and review its **Overview** page.
2. From the **Settings** menu, select **Networking**.
3. In the **Networking Overview** page, click the hyperlink next to **NIC Public IP** to display the properties of the NIC Public IP.
4. From the **Settings** menu, select **Configuration**.
5. Change **Assignment** from **Dynamic** to **Static**.
6. Enter the text for the **DNS name label**.
7. Click **Save**.

## 3.8 Increase the disk size

Microsoft Azure virtual machines are automatically given a default disk size of 64 GB.



The `root` and `/opt` partitions should be a minimum of 20 GB.  
`/var` should use a minimum of 80 GB for test environments and 200 GB for production environments.

When you have created and configured your VM using the Microsoft Azure Management Portal, you need to stop the VM and resize the disk.

You must wait for provisioning to finish, then:

1. Stop the VM.
2. Increase the disk size of the OS disk from the Portal. It is recommended that your disk size is large enough to accommodate two 20 GB partitions for `root` and `/opt`, and 200 GB for `/var`.



Other partitions (e.g. `usr`, `temp`, `home`, `boot`) may already be using up to 20 GB of disk space.

3. Start the VM.

## 3.9 Enlarge the OS partition

After increasing the disk size, you will need to resize the disk from the default size in Azure.

Follow the instructions at <https://docs.microsoft.com/en-us/azure/virtual-machines/linux/resize-os-disk-gpt-partition> for RHEL systems.

When the virtual machine has restarted, perform the following steps:

1. Access your VM as a root user by using the following command.

```
#sudo su
```

2. Use the `lsblk` command to determine which logical volume (LV) is mounted on the root of the file system. In the example below, it would be `rootvg-rootlv` in `sda4` which is currently reported as 63 GB.

```
[root@mail02-111-co-uk azureuser]# lsblk
NAME                                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda                                 8:0    0  128G  0 disk
├─sda1                             8:1    0   500M  0 part /boot/efi
├─sda2                             8:2    0   500M  0 part /boot
├─sda3                             8:3    0    2M  0 part
└─sda4                             8:4    0   63G  0 part
   ├─rootvg-tmplv                   253:0    0    2G  0 lvm  /tmp
   ├─rootvg-usrlv                   253:1    0   10G  0 lvm  /usr
   ├─rootvg-optlv                   253:2    0    2G  0 lvm  /opt
   ├─rootvg-homelv                  253:3    0    1G  0 lvm  /home
   ├─rootvg-varlv                   253:4    0    8G  0 lvm  /var
   └─rootvg-rootlv                  253:5    0    2G  0 lvm  /
sdb                                 8:16    0   32G  0 disk
└─sdb1                             8:17    0   32G  0 part /mnt
```

3. Use the `pvscan` command to determine which disk and partition holds the LVM physical volume or volumes (PV) in the volume group named `rootvg`. Note the size and free space listed between the brackets ([ and ]).

```
[root@mail02-111-co-uk azureuser]# pvscan
PV /dev/sda4   VG rootvg      lvm2 [<63.02 GiB / <38.02 GiB free]
Total: 1 [<63.02 GiB] / in use: 1 [<63.02 GiB] / in no VG: 0 [0  ]
```

4. Expand the partition that contains this PV by using `growpart`, the device name, and the partition number. This expands the specified partition to use all the free contiguous space on the device.

```
[root@mail02-111-co-uk azureuser]# growpart /dev/sda 4
CHANGED: partition=4 start=2054144 old: size=132161536 end=134215680 new: size=266381278 end=268435422
```

5. Use the `lsblk` command again to verify that the partition has been resized as expected. In the example below, `sda4` has changed from 63 GB to 127 GB.

```
[root@mail02-111-co-uk azureuser]# lsblk
NAME                                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda                                  8:0      0 128G  0 disk
├─sda1                              8:1      0  500M  0 part /boot/efi
├─sda2                              8:2      0  500M  0 part /boot
├─sda3                              8:3      0    2M  0 part
└─sda4                              8:4      0 127G  0 part
   ├─rootvg-tmplv                   253:0    0    2G  0 lvm  /tmp
   ├─rootvg-usrlv                   253:1    0   10G  0 lvm  /usr
   ├─rootvg-optlv                   253:2    0    2G  0 lvm  /opt
   ├─rootvg-homelv                  253:3    0    1G  0 lvm  /home
   ├─rootvg-varlv                   253:4    0    8G  0 lvm  /var
   └─rootvg-rootlv                  253:5    0    2G  0 lvm  /
sdb                                  8:16     0  32G  0 disk
└─sdb1                              8:17     0  32G  0 part /mnt
```

6. By using the `pvresize` command, expand the PV and use the rest of the newly expanded partition.

```
[root@mail02-111-co-uk azureuser]# pvresize /dev/sda4
Physical volume "/dev/sda4" changed
1 physical volume(s) resized or updated / 0 physical volume(s) not resized
```

7. Use the `pvscan` command again to verify that the new size of the PV is as expected. Compare the new size to the original [size / free] values.

```
[root@mail02-111-co-uk azureuser]# pvscan
PV /dev/sda4   VG rootvg      lvm2 [<127.02 GiB / <102.02 GiB free]
Total: 1 [<127.02 GiB] / in use: 1 [<127.02 GiB] / in no VG: 0 [0  ]
```

8. By using the output from the previous step, increase the size of the `root` partition as necessary. For example, if the `root` is currently 2 GB, run the following command to increase by 18 GB to 20 GB.

```
# lvresize -r -L +18G /dev/mapper/rootvg-rootlv
```



The `root` and `/opt` partitions should be a minimum of 20 GB.

`/var` should use a minimum of 80 GB for test environments and 200 GB for production environments.

9. Repeat the previous step to increase the size of the `/opt` and `/var` partitions as necessary. For example, if the `/opt` is currently 2 GB and the `/var` is 8 GB,

run the following commands to increase the sizes:

```
# lvresize -r -L +18G /dev/mapper/rootvg-optlv  
# lvresize -r -L +192G /dev/mapper/rootvg-varlv
```

10. Use the following commands to verify whether the logical volumes have an increased file system size.

```
#df -Th /  
#df -Th /opt  
#df -Th /var
```

## 4. Install Clearswift Secure Email Gateway

You can install the Clearswift Secure Email Gateway software using the following instructions.


### 4.1 Install from the Clearswift online repositories

To install Secure Email Gateway from repositories hosted online by Clearswift, you will need the Internet access to those repositories.

1. Assume root role at the command line.



When downloading and installing files, we recommend that you check the downloaded file can be verified against the vendor public key.

2. Download the packages containing the online repository configuration files.  
Click  below to open a page from where the commands can be individually copied and pasted into your terminal:



```
curl -Of https://products.clearswift.net/rhel7/seg/cs-rhel7-  
mirrors-22.02.04.rpm
```

```
curl -Of https://products.clearswift.net/rhel7/seg/cs-rhel7-  
email-repo-22.01.04.rpm
```

3. Download and install the Clearswift GPG public key:

```
rpm --import https://products.clearswift.net/RPM-GPG-KEY-  
Clearswift
```

4. Verify the downloaded packages:

```
rpm --checksig --verbose cs-*.rpm
```

This will display the results below, where all checks respond with OK:

```
cs-rhel7-email-repo-22.01.04.rpm:  
  
Header V3 RSA/SHA256 Signature, key ID 9c75f096: OK  
Header SHA1 digest: OK (6840df56446854f591490b64058734728a161f8c)  
V3 RSA/SHA256 Signature, key ID 9c75f096: OK  
MD5 digest: OK (7a0a8fde9b373bf35b261b95dda4798e)
```

```
cs-rhel7-mirrors-22.02.04.rpm:
```

```
Header V3 RSA/SHA256 Signature, key ID 9c75f096: OK
Header SHA1 digest: OK (172adf48c2225a2b7f433584ce6705655ad47137)
V3 RSA/SHA256 Signature, key ID 9c75f096: OK
MD5 digest: OK (55a611db509e4cf522bf98f93ec3d7b3)
```

5. Move Microsoft Update Repos from `/etc/yum.repos.d/` directory:

```
mv /etc/yum.repos.d/rh-cloud.repo /var/tmp
```

6. Manually install the downloaded repository file packages:

```
yum -y localinstall cs-*.rpm
```

7. Remove rsyslog:

```
yum -y remove rsyslog
```

8. Install the required product using the following command:

```
yum install -y cs-email --enablerepo=cs-*,ext-cs-*
```

This command temporarily enables access to the online repositories, and installs Secure Email Gateway.



If this step fails due to additional conflicts, you might need to remove the conflicting packages first using:

```
yum remove <package name>
```

## 4.2 Configure your Red Hat Enterprise Linux installation

If you used an SSH key when you created the Azure virtual machine, you will need to set a user password, using the following command:

```
passwd <username>
```

### Enable online repositories

Enable the online repositories using Red Hat Cockpit.

1. To access the Cockpit administration user interface, open a supported web browser and enter the IP address of your Secure Email Gateway, on port 9090:

<https://<ip-address>:9090>



2. Login using the administrator credentials, ensuring you have selected the **Reuse my password for privileged tasks** option.
3. Navigate to **Clearswift**. From **Product Actions > Enable online repositories**, click **Enable**.

### Create administrator accounts

Before you start using your Secure Email Gateway, we strongly recommend the following actions:

- Create a new administrator account to administer Secure Email Gateway
- Disable the root user account as a security precaution

This can be achieved using Red Hat Cockpit.

1. To access the Cockpit administration user interface, open a supported web browser and enter the IP address of your Secure Email Gateway, on port 9090:  
<https://<ip-address>:9090>
2. Login using the administrator credentials, ensuring you have selected the **Reuse my password for privileged tasks** option.
3. Navigate to **Accounts > Create New Account**.
  - Enter the name of the new administrator account and a strong password.
4. Click the new administrator account and enable the following role and policy:
  - Enable the **Server Administrator** role.
  - Select **Never lock account**. In the **Account Expiration** dialog, select **Never lock account** and click **Change**.
  - Select **Never expire password** or the **date** on which the password will expire. In the **Password Expiration** dialog, select **Never expire password** and click **Change**.
5. Log out of Cockpit and log back in using the new administrator credentials, ensuring you have selected the **Reuse my password for privileged tasks** option.
6. Navigate to **Accounts** and click the **root** user.
  - Select the **Lock Account** option to disable the root user.



It is good practice to create a secondary administrator account, just in case the password of the primary administrator account is lost. This can be achieved by repeating steps 4 and 5.

7. Navigate to **System** and **Restart** the Gateway.

## 4.3 Configure Secure Email Gateway

On restart, you will need to complete the Secure Email Gateway Installation Wizard.

1. To access the Secure Email Gateway interface, open a supported web browser and enter the IP address of your Gateway:  
`https://<ip-address>/Appliance`
2. Secure Email Gateway Installation Wizard is displayed.
3. Complete the wizard and click **Apply**.
4. The system might take around 5-10 minutes to apply the settings before you can use Secure Email Gateway. We recommend visiting the [First Steps](#) topic in the Online Help when the interface is accessible.

## 4.4 Configure update repositories

By default, the Clearswift online repositories are disabled after installation.

Switching from offline to online repositories gives access to Red Hat security fixes, normally within 24 hours of their publication and subsequent testing to ensure there are no compatibility issues. We recommend this for most installations.



The use of online repositories will download updates to your system. Microsoft will charge your Azure account for these transfers.

## 4.5 How to change your network settings

1. Use Red Hat Cockpit to configure an IP address.
2. Deploy network changes.
3. Use the Microsoft Azure Management Portal to set a static IP address to match the configuration.
4. Try to reconnect to your system after a few minutes.

Note that:

- The IP Address must belong to the **Virtual network** range you created earlier.
- Double check your settings before applying network configuration, as it is possible to lose connection with your virtual machine. Contact our Support if this occurs.
- Deploy network changes in Cockpit first, before replicating them in the Microsoft Azure Management Portal.

- The first IP address in your **Virtual network** range is your network gateway.
- After modifying your VM's IP address in the Microsoft Azure Management Portal, allow up to five minutes for Azure to apply the change. Azure might reboot your VM during this process.

## 5. Upgrade

---

If you are upgrading the current version of your Secure Email Gateway on Microsoft Azure, please refer to the [Installation and Getting Started Guide](#) for detailed instructions.

## Appendix A: Configure multiple NICs on Azure

---

You might require your installation to use multiple Network Interface Controllers (NICs). At present, you cannot configure this directly with the Microsoft Azure Management Portal.

However, you can install multiple NICs using Azure's CLI for PowerShell. This software communicates with the Microsoft Azure Management Portal using PowerShell.

You can download Azure's CLI for PowerShell from the Microsoft GitHub page. Look for Precompiled Installers.



For detailed instructions on using external resources, such as the Microsoft Azure Management Portal and the Microsoft GitHub page, refer to the appropriate documentation by the providers. Fortra is not responsible for changes to any of the procedure steps described.

The installation process is as follows:

1. Collect the resources you need to build a suitable virtual network.
2. Add in your NICs and associate them with your resources.
3. Configure the deployment of the operating system and virtual machine.
4. Start the VM and install the Gateway.

### Log in

When you have installed Azure's CLI for PowerShell, use the following procedure to log in to Azure.

Using a Windows Powershell Session:

1. Execute `azure login`. PowerShell displays a URL and a code.
2. Navigate to a web browser to the given URL and use the code provided.
3. Click **Continue** to log in to the Microsoft Azure Cross-platform Command Line Interface.

When connected, Azure displays either a login screen, or indicates that you are already connected.

### Collect and configure your resources

To create and start a suitable VM which handles multiple NICs, you need to gather specific resources and configure them appropriately using the Microsoft Azure Management Portal.

1. Add a new **Virtual Network**. Your virtual network will contain the resources required for your VM.
  - a. From the hub menu, click **(+) New > Networking > Virtual Network**.
  - b. Add a **Name**, an **Address Range** and a **Subnet**.
  - c. Select your **Subscription** details.
  - d. Add a **Resource Group** if required.



Resource Groups are containers for your virtual network resources.

- e. Select a **Location**. This should be the data center nearest to you.
  - f. Click **Create**.

Azure displays **Deployments succeeded** if your settings have been successfully deployed.
2. Create your **Network interface cards**.
  - a. From the hub menu, click **(+) New** and search for *Network interface* in the search box. Select and create your first network interface.
  - b. Add a suitable **Name**, for example, *NIC1*.
  - c. Select your **Virtual Network**. Azure gathers your **Subnet** information and populates the field.
  - d. Select a **Dynamic** address.
  - e. Leave **Network security group** configured as **None**.
  - f. Add your **Subscription** details, **Resource Group** and **Location**.
  - g. Click **Create**.

Azure displays **Deployments succeeded** if your settings have been successfully deployed.
  - h. Repeat the process by clicking **(+) New > Network interface**. Create your second network interface using the same Virtual Network you selected for the first. Add a suitable **Name**, for example, *NIC2*.
  - i. Click **Create**.

Azure displays **Deployments succeeded** if your settings have been successfully deployed.
3. Configure a **Network security group**. This enables you to add firewall rules to your virtual environment.

- a. Add a suitable **Name**.
- b. Add your **Subscription** details, **Resource Group** and **Location**.
- c. When deployed, use the (+) **Add** button to add **Inbound Security Rules** to allow SSH and HTTPS requests.



Each Inbound Security Rule requires a **Name** and a **Priority**. The priority controls the order in which the rules are applied. We recommend the Source is set to **Any**.

- d. Select either an **Allow** or **Deny** action for each rule as required.
  - e. Click **Create**.
4. Associate each **Network interface** with your **Network security group**.
- a. From the SETTINGS menu in the Network security group, select **Network interfaces**.
  - b. Click the (+) **Associate** button and select your primary NIC.  
Azure informs you that it is saving the network interface. Your NIC is then added to the list of associated Network interfaces.
  - c. Click the (+) **Associate** button and select your second NIC.  
Azure informs you that it is saving the network interface. Your NIC is then added to the list of associated Network interfaces.



You can associate a SubNetwork (containing all your network interfaces) with your Network security group.

5. Create a **Public IP Address**. The Public IP Address configures how external users connect with your virtual environment.
- a. From the hub menu, click (+) **New > Networking > Public IP Address**.
  - b. Add a suitable **Name**.
  - c. Select either a **Dynamic** or **Static** address, according to your requirements.
  - d. Add a **DNS label**.
  - e. Add your **Subscription** details, **Resource Group** and **Location**.
  - f. Click **Create**.  
Azure displays **Deployments succeeded** if your settings have been successfully deployed.
6. Associate your **Public IP Address** with your primary Network interface.

- a. From the hub menu, open your **Public IP Address** and click the **Associate** button above the Essentials window.
  - b. Use the **Resource type** menu to select Network Interface Card from the drop-down.
  - c. Select your primary Network interface.
  - d. Click **OK**.
7. Create a **Storage Account**. The storage account is a container for all your required disks and data.
- a. From the hub menu, click **(+) New > Storage account**.
  - b. Add a suitable **Name**.
  - c. Select the **Account kind** as **General purpose**, and the **Performance** as **Standard**.
  - d. Configure **Replication** and **Storage service encryption** according to your policy.
  - e. Add your **Subscription** details, **Resource Group** and **Location**.
  - f. Click **Create**.

Azure displays **Deployments succeeded** if your settings have been successfully deployed.

## Create your VM

When you have gathered all your resources, you need to configure the VM which will host your installation of Secure Email Gateway. The software runs on Red Hat Enterprise Linux (RHEL) 7.9.

You need the following information to complete this process:

### Required parameters

- **Location:** the location of the data center you selected earlier, for example, **UKSouth**.
- **Publisher:** RedHat
- **Offer:** RHEL
- **ID:** 7.9
- **Virtual Network Name:** the name you assigned to your Virtual Network
- **Subnet Name:** the name you assigned to your subnet
- **Resource Group Name:** The name you assigned to your Resource Group
- **NIC1:** the name you assigned to your primary Network interface
- **NIC2:** the name you assigned to your second Network interface
- **Storage Account Name:** The name you assigned to your Storage Account



1. Use PowerShell to gather all the versions of Red Hat 7.9 available in your Location.

```
azure vm image list Location RedHat RHEL 7.9
```

PowerShell displays a list of available images. The **Urn** column displays the unique reference of the latest available images.

2. Make a note of the latest **Urn** version (as shown) for later use. You will need all the characters after the final colon, for example: RedHat: RHEL: 7.9:7.9.20161213

- **Urn string:** 7.9.20161213

3. Use the following PowerShell command to find available disk sizes for your region:

```
azure vm sizes --location Location
```

```
PS C:\Users\ > azure vm sizes --location UKSouth
Info: Executing command vm sizes
+ Listing virtual machine sizes available in the location "uksouth"
data: Name CPU Cores Memory <MB> Max data-disks Max data-disk Size <MB> Max OS-disk Size <MB>
data: -----
data: Standard_A0 1 768 1 20480 1047552
data: Standard_A1 1 1792 2 21680 1047552
data: Standard_A2 2 3584 4 138240 1047552
data: Standard_A3 4 7168 8 291840 1047552
data: Standard_A5 2 14336 4 138240 1047552
data: Standard_A4 8 14336 16 619520 1047552
data: Standard_A6 4 28672 8 291840 1047552
data: Standard_A7 8 57344 16 619520 1047552
data: Basic_A0 1 768 1 20480 1047552
data: Basic_A1 1 1792 2 40960 1047552
data: Basic_A2 2 3584 4 61440 1047552
data: Basic_A3 4 7168 8 122880 1047552
data: Basic_A4 8 14336 16 245760 1047552
data: Standard_D1_v2 1 3584 2 51200 1047552
data: Standard_D2_v2 2 7168 4 102400 1047552
data: Standard_D3_v2 4 14336 8 204800 1047552
data: Standard_D4_v2 8 28672 16 409600 1047552
data: Standard_D5_v2 16 57344 32 819200 1047552
data: Standard_D11_v2 2 14336 4 102400 1047552
data: Standard_D12_v2 4 28672 8 204800 1047552
data: Standard_D13_v2 8 57344 16 409600 1047552
data: Standard_D14_v2 16 114688 32 819200 1047552
data: Standard_D15_v2 20 143360 40 286720 1047552
```

Make a note of the size you require, for example:

- **VM Size:** Standard D2 v2

4. Use the following PowerShell command to collect the resources you configured in the Microsoft Azure Management Portal:

```
$Network="$($azure network vnet subnet show --resource-group
Resource_Group_Name --vnet-name Virtual_Network_Name --name
Subnet Name | grep Id)".Split(":")[2].Trim()
```



Enter the Resource Group, Virtual Network Name and Subnet



Name *exactly* as you configured them in the Microsoft Azure Management Portal.

This command creates a new variable (*Network*) which includes a trimmed summary of all of your network information, as configured in the Microsoft Azure Management Portal.

### Create the VM using your parameters

Create the VM using all of the resources you have collected and prepared, including the **Urn string** and **VM Size** you recorded earlier. You also need to decide:

- **Virtual Machine Name:** A suitable unique name for your VM.
- **Container Name:** A suitable unique name for the container for your storage account.
- **VMVHD Name:** The unique VHD filename of your VM. This parameter must end with the extension `.vhd`
- **Admin User Name:** A suitable administrator user name. This must not match any existing Clearswift user names such as `cs-admin`.
- **Secure Admin Password:** This must be a strong password containing a minimum of 8 characters, a lower case character, an upper case character, a number character and a special character.

Use the following command:

```
azure vm create --resource-group Resource_Group_Name --name Virtual Machine Name --location Location --vm-size VM_Size --subnet-id $Network --disable-boot-diagnostics --os-type linux --nic-names "NIC1,NIC2" --storage-account-name Storage_Account_Name --storage-account-container-name Container Name --os-disk-vhd VMVHD Name --admin-username Admin User Name --admin-password Secure Admin Password --image-urn RedHat:RHEL:7.9:Urn_string
```

PowerShell looks up your resources based on the configuration in the Microsoft Azure Management Portal, and begins the creation process. It might take a few minutes to deploy your VM.

When complete, PowerShell displays:

```
vm create command OK
```

## Check Azure displays your VM

1. From the hub menu in the Microsoft Azure Management Portal, click **Virtual Machines**. Your Virtual Machine Name is displayed with a status:
  - **Creating**: PowerShell is still creating the VM.
  - **Running**: The VM has been successfully created and is running.
2. Follow the process from the [Install](#) chapter to complete the installation of the software.

## Contact Fortra

---

Please contact Fortra for questions or to receive information about Secure Email Gateway. You can contact us to receive technical bulletins, updates, program fixes, and other information via email or Internet.

## Fortra Support Portal

For additional resources, or to contact Technical Support, visit the [Fortra Support Portal](#).

For support issues, please:

- Check this guide's table of contents and topics for information that addresses your concern.
- Check the Knowledge Base in the Fortra Support Portal for information that addresses your concern.
- Gather and organize as much information as possible about the problem, including job/error logs, screenshots or anything else to document the issue.