FORTRA

Clearswift Secure Email Gateway Amazon Machine Image (AMI)

Version 5.6.0

Installation Guide

Copyright Terms and Conditions

202306070617

Contents

Before you begin

We recommend being familiar with Amazon Web Services (AWS) and Amazon Machine Images (AMI) before you deploy Secure Email Gateway.

In this guide, we use:

- AWS Marketplace to subscribe to the AMI
- Amazon Elastic Compute Cloud (Amazon EC2), and the Amazon EC2 console to launch the instance

> You must have an AWS account to complete all the steps described in this guide.

> We assume that your AWS Regions supports the new launch instance wizard which Amazon EC2 implemented in 2022. If your AWS Regions does not support the new wizard, instructions in this guide may not be applicable to you. In that case, you can use our previous guide as a reference.

Subscribe to the Secure Email Gateway AMI

Subscribe to the AMI from AWS Marketplace

1. Sign in to AWS Marketplace.
2. Locate the Secure Email Gateway product page.

   You can either:

   - type *Clearswift* in the search field
   - from the **Categories** menu, select **Infrastructure Software** > **Security**. Refine the search results further by selecting *Fortra* from the **Publisher** section

   ⓘ AWS offers AMIs on a subscription basis. Secure Email Gateway uses a BYOL (Bring Your Own License) model.

3. Select the product.
4. In the product page, check the information and click **Continue to Subscribe**.
5. In the **Subscribe to this software** page, check the information and click **Continue to Configuration**.
6. In the **Configure this software** page, select the following:

   - **Fulfillment option**: 64-bit (x86) Amazon Machine Image (AMI)
   - **Software Version**: 5.6.0
   - **Region**: an appropriate regional data center for your organization

   ⓘ AWS Regions may vary according to proximity and cost, and should be selected carefully.

7. In the **Configure this software** page, click **Continue to Launch**.
8. In the **Launch this software** page, select the **Launch through EC2** from the **Choose Action** drop-down menu and click **Launch**.
9. You are redirected to the Amazon EC2 console.

Launch the Secure Email Gateway instance

AWS customers are required to perform all the necessary security configuration and management of their EC2 machines. This includes OS patching and AWS firewall configuration. For further information, see https://aws.amazon.com/compliance/shared-responsibility-model/.

Initiate the launch instance wizard from the Amazon EC2 console

By following the previous steps, you should automatically be redirected from AWS Marketplace to the Amazon EC2 console.

Alternatively, you can access the Amazon EC2 console directly, click **Launch instance** in the dashboard, and configure your instance in the **Launch an instance** page.

Configure the Launch an instance page

Name and tags

You can tag the name of your instance.

1. In the **Name** field, enter a name for the instance.
2. Click **Add additional tags**.
3. Enter a corresponding **Key** and a **Value**, then click **Add new tag**.

Application and OS Images (Amazon Machine Image)

Specify an OS image (AMI) you are launching. This should be the AMI you have subscribed to.

Instance type

From the drop-down menu, select an instance type. There is a number of available options for building your machine.

Instance	vCPU	CPU Credits/hour	Mem (GiB)	Storage	Network Performance (GB/s)
t3.xlarge	4	96	16	EBS only	up to 5
t3.2xlarge	8	192	32	EBS only	up to 5
t3a.xlarge	4	96	16	EBS only	up to 5
t3a.2xlarge	8	192	32	EBS only	up to 5

Use an **xlarge** or larger instance for production workloads.

Key pair (login)

Select or create a key pair to ensure secure connection to your AMI.

Network settings

1. Click **Edit** in the **Network settings** panel.
2. From the **VPC** drop-down menu, select a VPC your instance belongs to.
3. From the **Subnet** drop-down menu, select an existing subnet from your VPC that matches your requirements.

   For further information on Amazon Virtual Private Cloud, see https://aws.amazon.com/vpc/ and its documentation.

4. From the **Auto-assign Public IP** drop-down menu, select **Disable**.
5. In the **Firewall (security groups)** and **Inbound security groups rules** sections, you can select a security group to control traffic for your instance.

   Use the following as a reference:

   - **Type** - SSH, **Port range** - 22, **Source type** - restrict access to your valid IP addresses
   - **Type** - SMTP, **Port range** - 25, **Source type** - anywhere
   - **Type** - HTTPS, **Port range** - 443, **Source type** - restrict access to your valid IP addresses
   - **Type** - TCP/UDP, **Port range** - 9090, **Source type** - restrict access to the Red Hat Cockpit UI

   When configuring security group **Source type**, make sure you set rules to allow access from known IP addresses only.

   SMTP should be left unrestricted.

6. Click **Advanced network configuration**, and expand the section. **Advanced network configuration** is available only when you select the subnet.
7. For the **Network interface 1**, enter an IP address in the **Primary IP** field, or leave the field empty for an auto-assigned IP address.
8. If you are deploying PMM, you need to add a second NIC. Click **Add network interface** and configure the parameters.

PMM (Personal Message Management) is a component of Secure Email Gateway that enables your end-users to personally manage their held messages.

Configure storage

Configure your device storage. The **Configure storage** panel has two viewing modes; **Simple** and **Advanced**.

With the **Simple** view, you can specify the size and type of the volume. To display all parameters, click **Advanced** and switch the view.

Use the default devices provided with the AMI. These have been specifically partitioned for the deployment of Secure Email Gateway.

You can increase the **Size (GiB)** but you should not change the **Device** or **Snapshot ID**.

Advanced details

Configure any additional parameters you require.

If you are launching multiple instances of Secure Email Gateway, and would like to peer them, you have to configure the following before you launch the instances:

- **Number of instances** in the **Summary** panel
- **User data** in the **Advanced details** panel

For detailed instructions, see the next chapter; Peering within the Gateways.

Launch your instance

Review your configuration in the **Summary** panel, and click **Launch instance**.

The user interface takes a few minutes to start.

Peering within the Gateways

You can deploy additional Secure Email Gateway instances to provide resilience and scalability. By peering your Gateways, you can manage them all from a single point.

On the **Launch an instance** page:

1. In the **Summary** panel, select a desired value for the **Number of instances** field.
2. Copy the following script, and paste it into the **User data** field in the **Advanced details** panel.

> You can copy the script by clicking ⧉ below. This will open a new browser window where the script can be copied from.

⧉

```
#!/bin/bash
```

```
NEWUUID=`uuidgen`
```

```
echo "machine.uuid=$NEWUUID" > /opt/cs-gateway/cfg/system-id.properties
```

```
xmlstarlet ed -L -u "/System/@uuid" -v "$NEWUUID" /var/cs-gateway/uicfg/system.xml
```

```
xmlstarlet ed -L -u "/System/PeerAppliances/Peer/@uuid" -v
"$NEWUUID" /var/cs-gateway/uicfg/system.xml
```

After you launch

Configure access to Red Hat Cockpit

Before you access the Secure Email Gateway's user interface, you must configure your Gateway's Linux user to access Red Hat Cockpit.

1. Access the SSH key pair.
2. Log in to the virtual machine using SSH, for example:

   ```
   ssh -i keyPair.pem ec2-user@<ip-address>
   ```

3. Create a password for the root user in order to access Cockpit, for example:

   ```
   sudo -i
   ```

   ```
   passwd
   ```

> 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`

Configure Secure Email Gateway

When you have launched your AMI, navigate to the Secure Email Gateway installation wizard.

> To access the Secure Email Gateway interface, open a supported web browser and enter the IP address of your Gateway:
>
> `https://<ip-address>/Appliance`

The installation process begins. For information on installation from this point onwards, refer to the Installation and Getting Started Guide, (Configuring Secure Email Gateway section).

Removing the AWS restriction on port 25

AWS blocks outbound traffic on port 25 by default, so you will not be able to send emails unless this restriction is lifted. You will need to request AWS to lift the restriction.

For further information, see https://aws.amazon.com/premiumsupport/knowledge-center/ec2-port-25-throttle/.

Upgrade

If you are upgrading your current version of Secure Email Gateway on AWS, refer to the Installation and Getting Started Guide for detailed instructions.