FORTRA

Clearswift Secure Email Gateway

Version 6.0.0

Installation Guide

(on Amazon Web Services)

Copyright Terms and Conditions

202412040733

Contents

1. 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.

2. 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 **View purchase options**.
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**: 6.0.0
   - **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.

3. 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 are 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

Instance	vCPU	CPU Credits/hour	Mem (GiB)	Storage	Network Performance (GB/s)
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 Group 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 name** or **Snapshot**.

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

See the Peering within the Gateways chapter of this guide for more information.

Launch your instance

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

The user interface takes a few minutes to start.

4. 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.

(Click ⧉ to open a page from where you can copy the commands and scripts.)

```
#!/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
```

5. After you launch

After the launch, you may need to perform some actions to set up your Secure Email Gateway, and then complete the Initial Setup Wizard.

> For information on installation from this point onwards, please also refer to the "Configure Secure Email Gateway" chapter in the Installation Guide.

Post-launch actions

We recommend the following after launching the instance, but before configuring the Secure Email Gateway's Initial Setup Wizard.

Configure access to Red Hat Cockpit

Before you access the Secure Email Gateway's web 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`

FIPS mode

If you wish to operate your Secure Email Gateway in FIPS mode, you need to configure it at this point. See the Appendix of this guide for more information.

If you are not using FIPS mode, you can skip this section.

Complete the Initial Setup Wizard

Once you have gone through the post-launch actions and have restarted Secure Email Gateway, run the Initial Setup Wizard.

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

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/.

Appendix: FIPS mode

Your Secure Email Gateway can operate in FIPS mode. This needs to be configured after you have launched an instance, but before completing the Secure Email Gateway's Initial Setup Wizard.

Enable FIPS mode

1. Access a command line terminal via SSH or Cockpit.
2. Execute the following:

   ```
   fips-mode-setup --enable
   ```

3. Reboot, then return to the Complete the Initial Setup Wizard section of this guide and continue.

> Once enabled, you cannot disable FIPS mode without reinstalling the Gateway.

For more information on FIPS mode, see the Online Help.

Contact Fortra

For more information about the Fortra's Clearswift products and cybersecurity solutions, please visit our website.

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

Fortra Support Portal

Fortra Support Portal offers various helpful resources, such as product documentation and knowledge articles. You can also contact our Technical Support, using 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.