

Installation Guide

Clearswift Secure Email Gateway Amazon Machine Image (AMI)

Version 5.4.0

Copyright Terms and Conditions

Copyright Help/Systems LLC and its group of companies.

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 HelpSystems is strictly prohibited. Excerpts and links may be used, provided that full and clear credit is given to HelpSystems with appropriate and specific direction to the original content. HelpSystems and its trademarks are properties of the HelpSystems group of companies. All other marks are property of their respective owners.

202109280406

Contents

| | |
|--|------------|
| Copyright Terms and Conditions | ii |
| Contents | iii |
| Before you begin | 1 |
| Installing your Gateway on AWS | 2 |
| Sign in and subscribe | 2 |
| Configure this software | 2 |
| Launch this software | 2 |
| Choose an instance size | 3 |
| Configure instance details | 3 |
| Add Storage | 4 |
| Add Tags | 4 |
| Configure Security Group | 5 |
| Key Pair | 5 |
| Launch your instance | 5 |
| Peering within the Gateways | 6 |
| After you launch | 7 |
| Configure access to Red Hat Cockpit | 7 |
| Removing the Amazon Restriction on Port 25 | 7 |

Before you begin

We recommend being familiar with Amazon Web Services, Amazon Machine Images (AMI), and the AWS Marketplace before you deploy a Clearswift Gateway AMI. You can find out more on getting started with AWS here:

<https://docs.aws.amazon.com/marketplace/latest/buyerguide/buyer-getting-started.html>



You will need to create or sign into an AWS Marketplace account before deploying the Clearswift Secure Email Gateway.

Installing your Gateway on AWS

Sign in and subscribe

1. Make sure you are signed into AWS Marketplace with your AWS Account credentials.



AWS Marketplace provides access to thousands of products, including AMIs for Clearswift and Helpsystems products. Use <https://aws.amazon.com/> to create an account or sign in.

2. Navigate to the Clearswift Secure Email Gateway product page. The **Product Overview** displays information about the Gateway.
3. Click **Continue to Subscribe**.



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

4. Click **Continue to Configuration**.

Configure this software

The page displays various implementation options for the software you have subscribed to.

1. Select the following:
 - **Delivery Method:** 64-bit (x86) Amazon Machine Image
 - **Software Version:** 5.4.0
 - **Region:** the appropriate regional data-centre for your organization



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

2. Click **Continue to Launch**.

Launch this software

There are two options for launching the software. We recommend using the Amazon Elastic Compute Cloud (EC2). EC2 is a web service that provides

scalable capacity for your machines.

Select **Launch through EC2**.

This loads the AMI into your AWS account and enables you to select your sizing requirements.

Choose an instance size

The **Choose Instance Type** page displays a number of available options for building your machine. You can select any of the following for either a test or production workload:

| Instance | vCPU | CPU Credits/hour | Mem (GiB) | Storage | Network Performance (GB/s) |
|-------------|------|------------------|-----------|----------|----------------------------|
| t3.large | 2 | 36 | 8 | EBS only | up to 5 |
| t3.xlarge | 4 | 96 | 16 | EBS only | up to 5 |
| t3.2xlarge | 8 | 192 | 32 | EBS only | up to 5 |
| t3a.large | 2 | 36 | 8 | 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 a **large** instance for a test environment and an **xlarge** instance for production workloads.

Configure instance details



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. You can find out more information here: <https://aws.amazon.com/compliance/shared-responsibility-model/>

1. Click **Next: Configure Instance Details**.

The **Configure Instance Details** page includes a number of configuration options.



Use the Getting Started with Amazon VPC for more detailed information.

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-getting-started.htm>



For information on how to achieve peering within the Gateways, please see the following section: [Peering within the Gateways](#)

2. In the **Subnet** section, choose an existing subnet from your VPC that matches your requirements.
3. Disable the **Auto-assign Public IP** using the drop-down (**use subnet setting (Disable)**).
4. In **Network**, enter an IP address in the **Primary IP** field, or leave the field empty for an auto-assigned IP address.
5. If you are deploying PMM you will need to add a second NIC.



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

6. Configure any additional options you require.

Add Storage

The **Add Storage** page enables you to configure your device storage settings.



Use the default devices provided with the AMI. These have been specifically partitioned for the deployment of the Clearswift Gateway . You can increase the **Size (GiB)** but you should not change the **Device** or **Snapshot ID**.

Add Tags

On the **Add Tags** page, you can tag the name of your instance. Add a corresponding key and a value, then **Add Tag**.

Configure Security Group

On the **Configure Security Group** page, you can select a security group to control traffic for your instance. Select the following, including port numbers:

- **SSH - 22**: Configure **Source** to restrict access to your valid IP addresses.
- **SMTP - 25**: Configure **Source** to **Anywhere**.
- **HTTPS - 443**: Configure **Source** to restrict access to your valid IP addresses.
- **TCP/UDP - 9090**: Configure **Source** to restrict access to the Red Hat Cockpit UI.



When configuring security group **Source**, make sure you set rules to allow access from known IP addresses only. SMTP should be left unrestricted.

Key Pair

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

Launch your instance


Click **Launch Instances**.

The UI takes a few minutes to start.

Peering within the Gateways

You can now deploy additional Secure Email Gateway instances to provide resilience and scalability. Your Secure Email Gateway can be peered together so that you can manage them all from a single point.

To do this:

1. On the **Configure Instance Details** page, select the desired value of **Number of instances**.
2. In the **Advanced Details** section (of the **Configure Instance Details** page), in the **User data** field, copy and paste the following script. You can do this by selecting the link ( icon) below. This will open a new page 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-gate-  
way/uicfg/system.xml
```

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

After you launch

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



To access the interface, open a web browser with the IP address as your Gateway UI, for example: `https://10.11.12.13`

The Clearswift Secure Email Gateway installation process begins. For information on installation from this point onwards, please refer to the [Installation and Getting Started Guide](#), section 3.3.

Configure access to Red Hat Cockpit

Before you access the Gateway UI, 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 interface, open a web browser with the same IP address as your Gateway UI, on port **9090**, for example: `https://10.11.12.13:9090/`

You have now installed your Gateway and you should follow the instructions in [Red Hat Cockpit](#) to complete the configuration process.

Removing the Amazon Restriction on Port 25

Amazon now block 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 ask Amazon to lift the restriction.

See <https://aws.amazon.com/premiumsupport/knowledge-center/ec2-port-25-throttle/> for more information.