

## **Installation Guide**

### **Clearswift Secure Email Gateway Amazon Machine Image (AMI)**

**Version 5.5.0**

## 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.

202212141206

# Contents

---

<b>Copyright Terms and Conditions</b> .....	<b>ii</b>
<b>Contents</b> .....	<b>iii</b>
<b>Before you begin</b> .....	<b>1</b>
<b>Installing Secure Email Gateway on AWS</b> .....	<b>2</b>
Sign in and subscribe .....	2
Configure this software .....	2
Launch this software .....	3
Choose an Instance Type .....	3
Configure Instance Details .....	3
Add Storage .....	4
Add Tags .....	4
Configure Security Group .....	5
Key Pair .....	5
Launch your instance .....	5
<b>Peering within the Gateways</b> .....	<b>6</b>
<b>After you launch</b> .....	<b>7</b>
Configure access to Red Hat Cockpit .....	7
Removing the AWS restriction on port 25 .....	7
<b>Upgrade</b> .....	<b>8</b>

## 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.

For further information on getting started with AWS, see <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 Clearswift Secure Email Gateway.

# Installing Secure Email 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 the 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 Secure Email Gateway.
3. Click **Continue to Subscribe**.



AWS offers AMIs on a subscription basis. 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:** 5.5.0
  - **Region:** an appropriate regional data center 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 Type

The **Choose an Instance Type** page displays a number of available options for building your machine.

1. 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.

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

## Configure Instance Details

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



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/>.



For further information on getting started with Amazon VPC, see <https://docs.aws.amazon.com/vpc/latest/userguide/vpc-getting-started.htm>.



For information on how to achieve peering within the Gateways, see [Peering within the Gateways](#).

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



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

5. Configure any additional options as required.
6. Click **Next: Add Storage**.

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

1. Configure options as required.
2. Click **Next: Add Tags**.

## Add Tags

On the **Add Tags** page, you can tag the name of your instance.

1. Add a corresponding key and a value, then **Add Tag**.
2. Click **Next: Configure Security Group**.

## 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 user interface takes a few minutes to start.



## Peering within the Gateways


---

You can now deploy additional Gateway instances to provide resilience and scalability. Your Gateways 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. Expand the **Advanced Details** section. Copy the following script and paste it into the **User data** field.



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-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 Secure Email Gateway installation wizard.



To access the interface, open a supported web browser and navigate to the IP address of your Secure Email Gateway:

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

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

### 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
```



Enter the following URL into a supported web browser to load the Cockpit administration user interface:

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

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

### 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 Clearswift Secure Email Gateway on AWS, refer to the [Installation and Getting Started Guide](#) for detailed instructions.