FORTRA

Clearswift Secure Email Gateway

Version 5.7.0

Installation & Getting Started Guide

Copyright Terms and Conditions

Contents

1. About this guide

This guide provides information for administrators installing Clearswift Secure Email Gateway onto a virtual machine or physical server. 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:

- New customers installing Secure Email Gateway for the first time.
- Existing customers upgrading from an earlier version of Secure Email Gateway to version 5.7.0.

2. Before installing

This section outlines prerequisites and considerations you need to make before installing Secure Email Gateway. Secure Email Gateway runs on 64 bit Red Hat Enterprise Linux (RHEL) 7.9. You can install the product on a physical server or virtual machine. See Prerequisites for more information on supported platforms.

2.1 Types of installation

You can install Secure Email Gateway using one of the following processes:

Installation process	Description	Where to start
Private cloud (e.g. VMware, Hyper-V and customer source hardware)	Applies to users installing the product from an ISO image that contains both RHEL 7.9 or above and the Clearswift software.	Installing from the ISO image
Public cloud (e.g. AWS, Azure or customer supplied OS)	Applies to users installing the product on an existing RHEL 7.9 platform.	Appendix A: Software Install Process
Customer supplied hardware	Applies to users deploying the product using their own hardware.	Configuring the Gateway

2.2 Prerequisites

Before installing, ensure that you have the following:

2.2.1 Hardware requirements

Your computer or virtual machine requires a minimum of 8 GB RAM and an 80 GB hard drive for use in testing and demonstration environments.

We recommend a minimum of 200 GB hard drive for use in a production environment based on your storage and processing requirements.

For a production environment, we recommend the following based on your storage and processing requirements where your Secure Email Gateway is configured so that your policy has:

- 1 anti-virus scanner
- Optical Character Recognition (OCR) disabled

Email type product	Estimated Throughput	CPU Cores/vCPU	RAM (GB)	Disk (GB)	Raid
Physical - Low Spec	Under 20,000 msgs/hour	2	16	200+	Optional
Physical -	75,000 msgs/hour	4	16	300+	Yes

Email type product	Estimated Throughput	CPU Cores/vCPU	RAM (GB)	Disk (GB)	Raid
High Spec					
Virtual - Low Spec	Under 20,000 msgs/hour	2	16	200+	Optional
Virtual - High Spec	75,000 msgs/hour	4	16	300+	Yes

> (i) We recommend increasing the size of the Disk by a minimum of 25% if you intend to store message-tracking data for 2 years.

2.2.2 Installation media

Ensure that you are using the correct version of the ISO image:

- EMAIL-5.7.0.iso

> After downloading the ISO image, it is recommended that an MD5/SHA hash is generated and compared to the published hashes from the download area.

After you download a copy of the ISO image from the online Clearswift product download area, there are a number of ways you can use it to install the software:

- Copying the ISO image to USB media. See Appendix C of this guide for instructions.
- Attaching the ISO image as a virtual DVD drive. This applies to virtual machines only.

2.2.3 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. Install Secure Email Gateway

You can install the Secure Email Gateway software from the ISO image that you downloaded from the Clearswift download area in the Fortra Community Portal.

> After you sign in to the Fortra Community Portal, go to **Downloads** > **My Product Downloads**. In the **Downloads** page, select **Clearswift** and find your product.

3.1 Install RHEL 7.9 and Secure Email Gateway from the ISO image

1. Connect the ISO image or USB device as a bootable device and power on the server.

   The **Welcome to Clearswift Email Solutions** menu should be displayed. If the load device can not be found, you might need to adjust your system boot sequence in the BIOS.
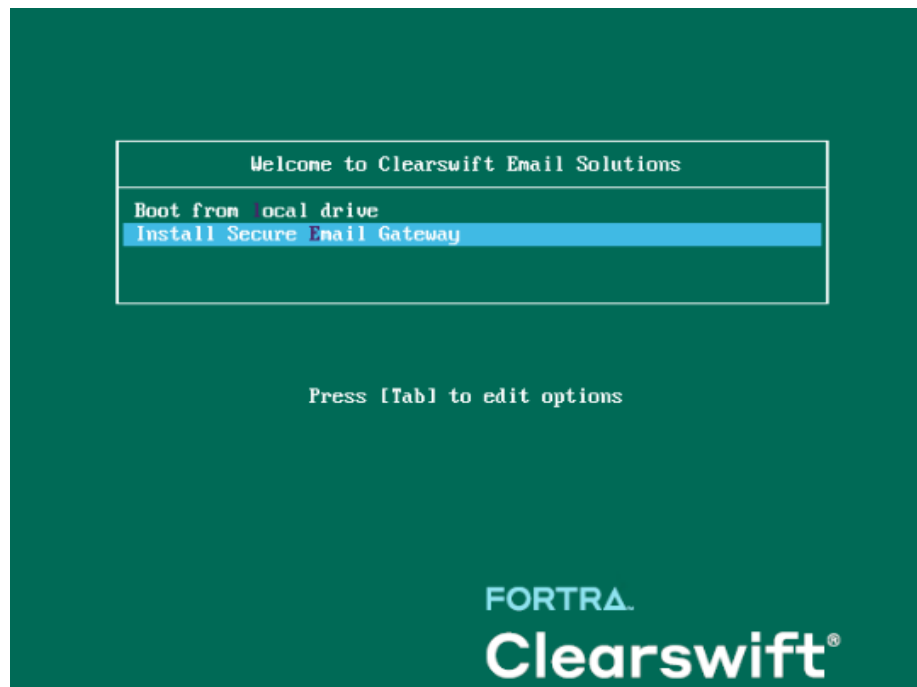
2. Use the arrow keys or keyboard shortcuts to select **Install Secure Email Gateway** from the menu. Press the **Enter** key to select the installation.

   The install process begins and starts the **Red Hat Installation Wizard**.

3. The **Red Hat Installation Wizard** is displayed and prompts you to select the language to be used during the installation process.

4. The wizard then begins the configuration of the server. Any of the settings may be changed but must be provided for any option marked with a warning ⚠ icon.

5. We recommend that you configure your network and host name settings now.

> By default, the network settings will be configured to use DHCP to obtain an IP address. If a DHCP server is not available you will be unable to continue unless a static IP address has been configured.

6. Scroll to the bottom of the wizard configuration page.

7. Click **Network and Host Name**.

8. Select the Network Card to configure and click **Configure**.

9. Select the **IPv4** Settings tab. Select **Manual** entry and click **Add**.

> We strongly recommend configuring each network card with a static network address.

10. Enter your network settings and click **Save**.

> Do not modify the **Device** field on the **Ethernet** tab as doing so could cause unexpected errors.

11. Enter your host name in the **Host name** field and click **Apply**.

3.2 Start the installation

1. Once satisfied that the host name and network cards are configured correctly, click **Begin Installation**.

2. During the installation process, you are prompted to set the root user password and create an additional administrator account.
   - We strongly recommend entering a strong password for root and any other users that are created.

3. You must create at least one additional user who is an administrator.
   - This can also be done post-installation via Red Hat Cockpit.
   - It is good practice to create a backup administrator user in case the primary administrator password is lost.

> Ensure that you keep a record of the password expiry for any created users as Red Hat does not automatically notify the user when the password is due to expire. If the administrator account becomes locked out, the only resolution is to take the system offline and boot into single user mode.

4. The package installation takes approximately 15-20 minutes to complete.
   - Once complete, the Red Hat Installation Wizard automatically reboots.

3.3 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.

> If the Clearswift installation media has been disconnected following the reboot, you must ensure that it is reconnected before configuring the Installation Wizard. The wizard requires access to the installation media to complete the setup of your Secure Email Gateway.

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.

3.4 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. Log in to Cockpit using the credentials created during the Red Hat installation, ensuring the **Reuse my password for privileged tasks** option is selected.

3. Navigate to **Accounts** > **Create New Account**.

   - Enter the name of the new administrator account and a strong password that meets the criteria defined in Appendix E: Password Policy.

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.

3.5 Configure update repositories

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

This means that any updates will need to be installed using the ISO of subsequent Secure Email Gateway releases.

Alternatively, if Secure Email Gateway has access to the Internet, it can receive updates from the online repositories.

- Switching from offline to the 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.

- However, you should only do this if you intend to also use the online repositories for future product upgrades.

> ⓘ Be aware that enabling the online repositories is an irreversible action.

The online repositories can be enabled by following the steps below:

1. Enter the Cockpit URL into a supported web browser to load the Cockpit administration user interface. Then login using the administrator credentials, ensuring you have selected the **Reuse my password for privileged tasks** option.

2. Navigate to **Clearswift**. From **Product Actions** > **Enable online repositories**, click **Enable**.

4. Upgrade from Secure Email Gateway 5.x

(i) If you are installing Secure Email Gateway for the first time, you can ignore this section.

The method used for upgrading from version 5.x depends on whether you are upgrading from the ISO or online repositories.

4.1 Upgrade from ISO

Use Cockpit to install the upgrade from the version 5.7.0 ISO image.

You must make the version 5.7.0 ISO image available to your Secure Email Gateway, noting that there is an ISO image per product.

If you are using a DVD and if it does not mount automatically, you may have to type the following at the command-line:

```
mount -r /dev/cdrom /media/os
yum clean all
```

4.2 Upgrade from online repositories

Follow the steps detailed in the Future updates section.

(!) After the upgrade, you will find that your upgrade mode has been reset to "offline".

In Cockpit, navigate to **Clearswift**. From **Product Actions** > **Enable online repositories**, click **Enable**.

4.3 Peer support

When upgrading your Secure Email Gateway, the following peer support rules are applicable:

- Secure Email Gateway version 5.7.0 (or earlier) can peer with another Secure Email Gateway version 5.7.0.
- Peer groups with mixed versions can co-exist with older versions to share message tracking, reporting and other peering features, but policy may not be applied remotely.

> (i) If you are using greylisting, your peer group should not contain peers prior to version 5.2.0 due to incompatibility between releases.
>
> If you own Secure Email Gateway of a version prior to 5.2.0, we advise that you un-peer your Secure Email Gateway prior to upgrading, and re-peer after upgrade.

4.4 Post-upgrade actions (after upgrading from version 5.x)

Following an upgrade of Secure Email Gateway, see Post-upgrade actions for important considerations and requirements .

If you are using the sandboxing feature, following an upgrade, you must also reapply the proxy configuration in Cockpit in order for sandboxing to recognize the proxy setting.

4.4.1 Reapplying the proxy configuration for use with sandboxing

> (i) This section can be ignored if you are not using the sandboxing feature.

1. In Cockpit, navigate to **Network Services** and click the **System Proxy** tab.
2. Click 🖊 **Edit**.
3. In the **Edit System Proxy** dialog, click **Apply**. You do not need to change any of the current settings.

> 💡 As part of the upgrade to version 5.4.3 or later, the URLs for sandboxing are updated from `https://XXXX.sandbox.sophos.com` (XXXX is a location of user's choice) to `https://XXXX.analysis.sophos.com`. The change will occur automatically upon upgrading.

5. Upgrade from Secure Email Gateway 4.x

> **(i)** If you are installing Secure Email Gateway for the first time, you can ignore this section.

> **(!)** **Upgrading from Secure Email Gateway version 4.x**:
> 1. Firstly, upgrade your version 4.x Gateway to version 5.2.0, following instructions in this section.
> 2. Secondly, upgrade your version 5.2.0 Gateway to version 5.7.0, following instructions in the Upgrading from 5.x section.

5.1 Preparation for upgrade

Before you attempt any kind of upgrade, you are advised to do the following:
1. Apply any pending configuration changes.
2. Clear all message queues.
3. Back up your system and latest configurations before installing.

5.2 Unsupported environments

The in-place upgrade of Red Hat 6 to 7 is not supported on the following platforms:

- Amazon Web Service (AWS) instances or Machine Images
- Microsoft Azure
- Microsoft Hyper-V
- Systems using a UEFI boot loader
- Systems using Integrated Dell Remote Access Controller (iDRAC)

If you are hosting your Secure Email Gateway software on one of these, refer to Appendix B: Resolving Upgrade Failures for further information.

5.3 Check prerequisites

> **(!)** 4.11.2 is minimum version required to upgrade to version 5.2.0.
>
> You will also need to download a copy of the version 5.2.0 ISO to complete an upgrade from version 4.11.2. See Prerequisites for more information.

To upgrade your Secure Email Gateway to version 5.x, you need to do the following:

1. Using the Clearswift Server Console, upgrade your Secure Email Gateway 4.x server to version 4.11.2 using the standard upgrade previously used to upgrade Secure Email Gateway 4.x servers.

   - This update will install the tools required to check if the server meets the necessary pre-requisites to run Red Hat 7.8 or above, to allow you to optionally perform the upgrade of Red Hat 7.9 and Secure Email Gateway software if met.

   - Follow the upgrade instructions in the version 4.11.2 Installation and Getting Started Guide so that your Secure Email Gateway is correctly configured before attempting to upgrade to version 5.2.0.

   On completion of the 4.11.2 upgrade, you will be ready to upgrade to Red Hat 7.9 and Secure Email Gateway 5.2.0.

2. From the Clearswift Server Console, open a Terminal Session and enter the following to assume root user privileges:

   ```
   sudo su
   ```

3. Check your Secure Email Gateway version 5.2.0 Installation media is accessible:

   ```
   ls /media/os/cs-iso-repo
   ```

   If your installation media is not available, enter the following command and then repeat the command above:

   ```
   service autofs restart
   ```

4. Start the upgrade verification process by entering the following command:

   ```
   cs-gateway-v5-upgrade.sh
   ```

5. The upgrade process will be performed in three phases:

   - **Analyze Gateway** will check the server meets the necessary pre-requisites to upgrade Red Hat 6 to Red Hat 7.9

   Assuming the pre-requisites are met, the following phases will be run to upgrade the software:

   - **Upgrade Red Hat** will perform the migration of Red Hat 6 to Red Hat 7.9

   - **Upgrade Gateway** will upgrade Secure Email Gateway 4.x software to 5.x

```
Welcome to the Clearswift Gateway v5.0 Upgrade

During this upgrade, both the Red Hat Operating System and existing Gateway software will
be upgraded. This will be performed in the following phases:

Phase                                             Status
---------------------------------------------------------------------------------------
1. Analyze Gateway                                Not Started
2. Upgrade Red Hat                                Not Started
3. Upgrade Gateway                                Not Started

Throughout this upgrade, your Clearswift SECURE Gateway V5 ISO must be available.

The full upgrade process could take several hours to complete.

Are you ready to continue (y/n)? _
```

6. Enter **y**(es) to start the upgrade process. You will be prompted to select if you
    want to:

    - Check if the Gateway can be upgraded but upgrade later

        ○ This is useful if you want to understand what steps you will need to
          plan for before you are ready to upgrade

    - Check if the Gateway can be upgraded and upgrade now

```
Before the Gateway can be upgraded an analysis will be run; this can take several hours.

You can choose to upgrade the Gateway without further intervention, or to just perform
the analysis and do the upgrade later.

Please choose:

    0 - exit now
    1 - only run the analysis
    2 - run the analysis and upgrade the Gateway if possible

Please enter 0 to exit, 1 to analyse or 2 to upgrade:  _
```

7. Presuming you have entered option 1 or 2 at the prompt, the Red Hat analysis
    process begins.

> ⊙ This process can take several hours to complete. Do not restart
> your Secure Email Gateway while it is under analysis.

At the end of the process, you will be notified if the server can or cannot be
upgraded to Red Hat 7.9.

> (!) In the event of your Secure Email Gateway not meeting the necessary pre-requisities to be upgrade, refer to Appendix B: Resolving Upgrade Failures.

5.4 Upgrade Secure Email Gateway

Follow the steps below to continue upgrading Red Hat 6 to 7.9.

1. If you selected to analyze only, but have decided to continue with the upgrade, you can restart the upgrade by entering the following command line:

```
cs-gateway-v5-upgrade.sh
```

2. The upgrade process will prompt you to reset the root user password.

> (!) You must reset the root password unless you know the existing password and have verified you can login to this server using it.
>
> This is temporarily required to allow you to log in to Red Hat Cockpit and create new administrator account(s) that you will then use to administer Secure Email Gateway from a Terminal session.

Once you have created these new accounts, you are strongly recommended to disable the root user account as a security precaution.

> (!) The cs-admin user that you would have used to administer Secure Email Gateway from a version 4.x Terminal Session is no longer available in Secure Email Gateway version 5.0.0 onwards.

3. The upgrade of Red Hat 6 to 7.9 will now begin. The server will reboot midway through and then complete the upgrade during the server restart.

> (i) Make sure your installation media is connected.

4. The upgrade process should take between 15-30 minutes. During this time, your Gateway will automatically reboot several times. You can access the Secure Email Gateway Web UI once the upgrade is complete.

5.5 Post-upgrade actions (after upgrading from version 4.x)

The Red Hat and Secure Email Gateway upgrade process should now have completed.

You can verify this by logging into the terminal session using your root user credentials and entering the following command:

```
cs-gateway-v5-upgrade.sh
```

After the final reboot, there will be a delay of approximately 10 minutes whilst the Gateway initializes.

5.5.1 Run a system connectivity test

Following a system upgrade, we recommend that you run the **Connectivity Test**. The test checks that the upgraded system is still capable of accessing all external resources such as AV update mirrors, DNS and similar.

> (i) To access the test, navigate to the **System** menu and select one of the sub menus, such as **Ethernet Settings** and **SSH Access**. Then, click the **Connectivity Test** in the task panel.

5.5.2 Create new administrator account(s)

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

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

See Creating administrator accounts for further information.

> (!) The "cs-admin" user account previously used in the Gateway 4.x is not supported. You must use a new administrator account instead.

5.5.3 Applying the DISA STIG security profile

The DISA STIG security profile is not applied during an upgrade. To apply this profile following an upgrade see Appendix F for further instructions.

5.5.4 Re-join domains

If you have previously joined the Gateway to a domain controller to use features such as the PMM Portal, you must re-join each domain before using those features.

5.5.5 Future updates

You will be notified of future updates in the Secure Email Gateway administration UI and via 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. Navigate to **Software Updates** and click **Check for Updates**.

See Configuring update repositories for instructions on how to enable the online repositories if you would like to retrieve updates from those repositories.

> (i) **Online repositories or Offline mode?**
>
> Offline mode is designed for installations that operate in a closed environment, disconnected from the Internet. Unless this is a very specific requirement for your system, you should upgrade Secure Email Gateway from the online repositories.
>
> To perform an offline upgrade, you require a copy of the latest release ISO mounted to suitable media (for example, USB). Please contact our Support if you need additional guidance on how to complete this step.

Appendix A: Software install process

The following steps describe how to install Secure Email Gateway on top of an existing Red Hat Enterprise Linux (RHEL) 7.9 Server (including a suitably configured AWS or Azure instance).

> (i) You should install Red Hat 7.9 as a **Minimal** server installation, with a separate `/(root)` and `/var` partition.
>
> The `root` partition should be a minimum of 20 GB, and the `/var` partition should use a minimum of 80 GB for test environments and 200 GB for production environments.

> (i) If you want to secure your Red Hat 7.9 Server to DISA STIG Compliance standards, you will need to apply this profile before you continue with the Secure Email Gateway installation. See Appendix F for details.

Install from the Secure Email Gateway ISO

To install Secure Email Gateway:

1. Open a Terminal and login as root user.

2. Insert the media containing the ISO image and mount it onto /media/os:

```
mkdir -p /media/os
mount /dev/cdrom /media/os
```

3. Import the Clearswift GPG public key:

```
rpm --import /media/os/RPM-GPG-KEY-Clearswift
```

4. Install the cs-media package. The cs-media package configures your system to be ready for you to install the Gateway from the ISO image:

```
yum install -y /media/os/cs-iso-repo/cs-media*.rpm
```

5. If you intend to update from the Clearswift online repositories in the future, enter the following to install the required configuration files:

```
yum install -y cs-rhel7-email-repo cs-rhel7-mirrors
```

6. Install the required product using the following command:

```
yum install -y cs-email
```

> ⓘ If this step fails due to additional conflicts, you might need to remove the conflicting packages first using:
> ```
> yum remove <package name>
> ```

7. Reboot the Gateway, and then continue from <u>Configuring Secure Email Gateway</u>.

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. Manually install the downloaded repository file packages:

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

6. 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.

> (i) If this step fails due to additional conflicts, you might need to remove the conflicting packages first using:
> ```
> yum remove <package name>
> ```

7. Enable the online repositories. See Configuring Update Repositories for more information.

8. Reboot the Gateway, and then continue from Configuring Secure Email Gateway.

Post installation considerations

1. All system administration actions should be performed using Red Hat Cockpit.

   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
   ```

> You should avoid changing network configuration at the command line as Secure Email Gateway is is not notified of these changes.
>
> If changing network configuration at the command line is necessary, please contact our Technical Support for more information.

2. If you want to secure your Secure Email Gateway using the DISA STIG security profile, see Appendix F for further instructions.

3. The Firewall configuration will be controlled via the Secure Email Gateway administration user interface. If SSH access is required you need to re-enable it through the user interface. See SSH Access in the Online Help for more information.

4. The crontab configuration is modified. Pre-existing root cronjobs might be lost, but you can re-add them.

Install additional software

The software installation process will not automatically disable any of your pre-existing repository configurations. From the command line you will be able to install additional third-party software in the normal way. This includes additional Red Hat software.

> You will only be able to apply Clearswift-provided upgrades via Cockpit. This ensures that only trusted Clearswift repositories are used during the upgrade process, and any unintended updates from third-party repositories will be blocked during the process.

Appendix B: Resolve upgrade failures

If you are unable to perform an in-place upgrade of your Secure Email Gateway using the instructions in Upgrading from version 4.x, the following sections provide you with some options on how to upgrade or migrate your existing policy.

Secure Email Gateway does not meet Red Hat 7.9 pre-requisites

If the upgrade failed because your Secure Email Gateway did not meet the Red Hat pre-requisites for upgrading to Red Hat 7.9, you should review the analysis report:

`/var/log/cs-gateway/upgrades/redhat-pre-upgrade-report.txt` (or .html)

This report will tell you the exact reasons for the failure, and in some cases provide helpful tips on how to resolve the problems.

Restoring version 4.11.1 (or later) backup to Secure Email Gateway 5.x

If you are unable to resolve the issues preventing you from performing an in-place upgrade, you can instead install a new Secure Email Gateway 5.x server and then restore a backup from Secure Email Gateway 4.11.1 or later.

> ⓘ Restoring a version 4.11.1 backup (or later) does not automatically restore the peer group roles so they must be restored manually.

> ⓘ It is not possible to restore a version 4.11.1 system backup on Secure Email Gateway later than version 5.3.0.

Restoring peer group roles

There are two ways by which peer group roles can be restored.

Using PMM

1. Navigate to **System** > **PMM Settings** > **Portal Settings**.
2. In the **Peer Roles within PMM** panel, ensure the **Enable Portal** and **Enable Digest** options are each assigned to a peer.

Using a Trust Center

1. Navigate to **System** > **Encryption** > **Trust Center Configuration**.

2. In the **Automatic Certificate Generation** panel, ensure that at least one peer has been assigned for the role.

> See [Backup and Restore the system](#) in the Online Help for more information.

Appendix C: USB installation media preparation

The following steps describe how to copy the Secure Email Gateway software ISO image to USB media.

1. Download the Secure Email Gateway software ISO image from the Clearswift download area in the Fortra Community Portal.

    > After you sign in to the Fortra Community Portal, go to **Downloads** > **My Product Downloads**. In the **Downloads** page, select **Clearswift** and find your product.

    > After downloading the ISO image, it is recommended that a MD5/SHA hash is generated and compared with the published hashes from the download area.

2. Download a USB tool that maintains drive volume name. We recommend using Rufus Portable.

    > Do not use the standard version of Rufus for this process. Ensure that you use the portable version.

    > Although you can use USB tools other than Rufus, the following USB tools will not work with the Secure Email Gateway software ISO image:
    > - YUMI
    > - Universal USB Installer
    > - Fedora liveusb-creator

3. Assuming that you are using Rufus 3.11 Portable, run **rufus-3.11p.exe**.

4. Insert your USB media and select it from the **Device** drop-down menu.

5. Under **Boot Selection**, click **SELECT** to select the ISO you want to burn. Once Rufus scans the ISO, it fills in other options automatically.

> ⓘ When you burn the ISO, the volume label must be called CS_ RHEL_GW.

6. Click **Start**. The **ISOHybrid image detected** dialog box appears. Select **Write in ISO Image mode (Recommended)** and then click **OK**. A dialog box appears to warn you that any existing drive date will be removed. Click **OK** if you are happy to proceed.

7. Return to Installing Secure Email Gateway to complete the installation process.

Appendix D: Firewall ports

You might need to open the following ports on your DMZ firewall, depending on your network configuration:

Port	Protocol	Direction	Required for
20	FTP	In/Out	Backup & Restore if using an FTP server located beyond the firewall.
21	FTP	In/Out	Backup & Restore and Transaction Logging if using an FTP server located beyond the firewall.
21	FTPS (exp)	In/Out	Backup & Restore and Transaction Logging.
22	TCP	In	SSH access to the console.
22	SFTP	Out	Backup & Restore, and, server containing lexical data for import
25	TCP	In	Inbound SMTP
25	TCP	Out	Outbound SMTP. If your system uses an alternative port, open that instead.
53	UDP/TCP	In/Out	TRUSTmanager LiveFeed checks
53	UDP/TCP	Out	DNS requests, if using DNS servers beyond the firewall. Only allow outbound requests to the specified DNS servers, and responses from those servers.
80	TCP	In	HTTP access to the PMM interface (if using PMM)
80	TCP	Out	HTTP access to the Clearswift Junk Email and Malware Detection Servers
80	TCP	Out	HTTP access to the policy rule/engine and spam update servers
80	TCP	Out	Clearswift Spam Detection stats from: **clearswiftstat.mailshell.net**
80	TCP	Out	Access to SpamLogic Rule/Engine updates: **sn12.mailshell.net** **db11.spamcatcher.net** **verio.mailshell.net** **ruledownloads.mailshell.net** **tisdk.mailshell.net**
80	TCP	Out	HTTP access to Secure Email Gateway online help
80	TCP	Out	Access to the Service Availability List:

Port	Protocol	Direction	Required for
			services1.clearswift.net services2.clearswift.net services3.clearswift.net
80	TCP	Out	Access to the RSS Feed from: www.clearswift.com
123	UDP	In/Out	Access to NTP services, if configured. The following servers are configured by default: 0.rhel.pool.ntp.org 1.rhel.pool.ntp.org 2.rhel.pool.ntp.org 3.rhel.pool.ntp.org
135	TCP	Out	User authentication using NTLM (when using PMM in Full Mode)
137	UDP	Out	User authentication using NTLM (when using PMM in Full Mode)
139	TCP	Out	User authentication using NTLM (when using PMM in Full Mode)
161	UDP	Out	SNMP inbound: the port used by an SNMP browser when scanning Secure Email Gateway
162	UDP	Out	SNMP alerts
389	TCP	In/Out	LDAP directory access (if you use LDAP servers beyond the firewall)
389	TCP	In/Out	LDAP Key Server Queries
443	TCP	In/Out	HTTPS Key Server Queries
443	TCP	In/Out	HTTPS access to Clearswift Secure Email Gateway web interface and for communications between Peer Gateways
443	TCP	Out	HTTPS access to the Clearswift Update Server for TRUSTmanager statistics.
443	TCP	Out	HTTPS MTA-STS policy file queries
443	TCP	Out	HTTPS access to the Clearswift Update Server for license management and handling Managed Lexical Expression Lists: applianceupdate.clearswift.com

Port	Protocol	Direction	Required for
443	TCP	Out	Access to Clearswift product and Operating System updates: **products.clearswift.net** **rh7-repo.clearswift.net**
443	TCP	Out	HTTPS access to the Sophos or Avira Update Servers for fetching anti-virus updates and software upgrades. Sophos update servers: **sav-update-1.clearswift.net** **sav-update-2.clearswift.net** **sav-update-3.clearswift.net** **sav-update-4.clearswift.net** **sav-update-5.clearswift.net** **sav-update-6.clearswift.net** Avira update servers: **aav-update-1.clearswift.net** **aav-update-2.clearswift.net** **aav-update-3.clearswift.net** **aav-update-4.clearswift.net** **aav-update-5.clearswift.net** **aav-update-6.clearswift.net** ***.apc.avira.com**
443	TCP	Out	HTTPS access to Sophos Sandboxing Server (port is used for sending potential malware for scanning, and this traffic must not be blocked): **analysis.sophos.com** **apac.analysis.sophos.com** **au.analysis.sophos.com** **de.analysis.sophos.com** **uk.analysis.sophos.com** **us.analysis.sophos.com**
443	HTTP/S	Out	Access to Sophos URL Lookup Server: **4.sophosxl.net**
443	TCP	Out	Access to the SpamAssassin ruleset database: **spamassassin.clearswift.net**
443	TCP	Out	Access to the PhishTank URL database:

Port	Protocol	Direction	Required for
			phishtank.clearswift.net
445	TCP	Out	User authentication using NTLM (when using PMM in Full Mode)
514	TCP	Out	Access to the central SYSLOG server (log export)
636	TCP	In/Out	Secure LDAP/S directory access
990	FTPS	In/Out	Backup & Restore and Transaction Logging.Also used to connect Clearswift Secure Email Gateway with your server containing lexical data for import.
3268	TCP	Out	LDAP connection to an active directory global catalog port (if you are using LDAP servers beyond the firewall)
3269	TCP	In/Out	LDAP and SSL connection to an active directory global catalog port (if you are using LDAP servers beyond the firewall)
9090	TCP	In/Out	Connection to Red Hat Cockpit
11371	TCP	In/Out	HTTPS Key Server Queries
19200	UDP	In/Out	Broadcasting of greylisting data to Peer Gateways

Appendix E: Password policy

The default password policy applied after the Secure Email Gateway installation uses specific rules from the DISA STIG security profile. This is the same for all installation methods. For non-ISO installs, extra steps will still need to be followed in order to apply the rest of DISA STIG profile if required. See Appendix F for further details

Policy	Required
The minimum number of required classes of characters for the new password (uppercase, lowercase, digits, non-alphanumeric characters)	4
The minimum acceptable size for the new password	15
The minimum number of upper case characters in the password	1
The minimum number of lower case characters in the password	1
The minimum number of digits in the password	1
The minimum number of non-alphanumeric characters in the password	1
The maximum number of allowed consecutive characters of the same class in the new password	4
The maximum number of allowed consecutive same characters in the new password	3
The maximum number of characters in the new password that can be reused from the old password	8
Prevent use of dictionary words	true

> (i) Refer to your organization's own best practices and recommendations when creating suitable passwords that meet Clearswift's password policy.

Appendix F: How to apply the DISA STIG security profile

The Defense Information System Agency (DISA) publishes Security Technical Implementation Guides (STIG) which describe how to securely configure various computer systems and software.

> ⚠ Before applying this security profile, please be aware that the performance of traffic-processing on your Secure Email Gateway could be reduced.
>
> This is due to the increase in the level of auditing performed by the Red Hat audit service. We recommend that you carefully monitor performance before and after applying the profile, and assign additional hardware resources if required.

Installing via the Secure Email Gateway ISO

If you have installed your Secure Email Gateway using the ISO Image, the DISA STIG security profile is automatically applied for Red Hat 7.9. This is implemented using Open Security Content Automation Protocol (OSCAP).

Installing via the Software install process

For the Software install process, you will need to apply the DISA STIG security profile to your Red Hat 7.9 Server both before and after Secure Email Gateway has been installed.

Upgrading a previous Secure Email Gateway

If you upgraded from a previous version of Secure Email Gateway, follow these instructions to apply the DISA STIG security profile:

For the upgrade process, you only need to apply the profile after the upgrade has completed. See Applying profile after the Secure Email Gateway installation.

Applying profile before the Secure Email Gateway installation

The following steps will apply the security profile to your server before you install Secure Email Gateway using the Software install process.

1. Open the terminal on your Red Hat 7.9 server.

2. Login as the root user.

3. Install the following packages:

```
yum -y install scap-security-guide
```

4. Execute this command to apply the security profile:

```
oscap xccdf eval --remediate --profile xccdf_org.ss-
gproject.content_profile_stig --report /tmp/disa-stig-
report.html /usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
```

5. You can check the level of compliance that has been applied by viewing:
   `/tmp/disa-stig-report.html`.

6. Reboot the system in order for the DISA STIG security profile modifications to be applied.

Applying profile after the Secure Email Gateway installation

The following steps will re-apply the security profile to your server after installing Secure Email Gateway.

1. If you have not enabled online repositories, insert your Secure Email Gateway ISO.

2. 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`

3. Log in to Cockpit using the credentials for your administrator account, ensuring the **Reuse my password for privileged tasks** option is selected.

4. Navigate to **Terminal**. Assume root user privileges using the following command:

```
sudo su
```

5. Execute the following script and wait for it to complete:

```
/opt/clearswift/platform/stig/bin/remediate-disa-stig.sh
```

6. Once the script has completed, you must reboot the system in order for the DISA STIG security profile modifications to be applied.

Evaluating Secure Email Gateway

To evaluate the DISA STIG Compliancy rating of your Secure Email Gateway, you can generate a report by following these instructions:

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. Log in to Cockpit using the credentials for your administrator account, ensuring the **Reuse my password for privileged tasks** option is selected.

3. Navigate to **Terminal**. Assume root user privileges using the following command:

```
sudo su
```

4. Execute the following script:

```
/opt/clearswift/platform/stig/bin/evaluate-disa-stig.sh
```

5. The report will be available from:

```
/var/opt/clearswift/platform/stig/disa-stig-results.html
```

> If you wish to validate your DISA STIG compliance, please contact our Support and request a compliance document.