clearswift
by HelpSystems

Installation & Getting Started Guide
Clearswift Secure Exchange Gateway

Version 5.1.0

Copyright Terms and Conditions

Contents

1. About this guide

This guide provides information for administrators installing the Clearswift Secure Exchange Gateway onto a virtual machine or physical server. It covers the procedures and requirements necessary for a full installation.

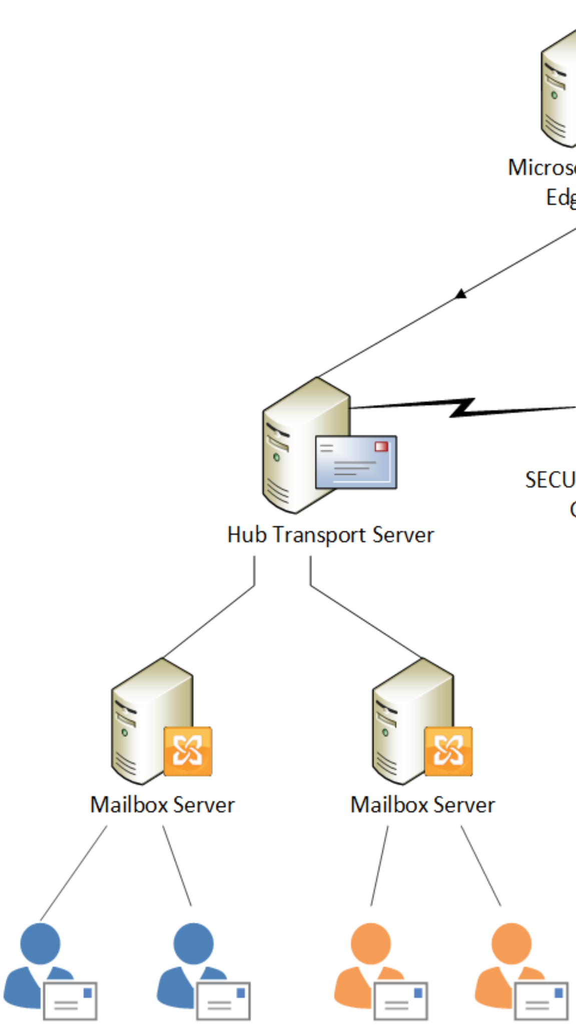
1.1 Who is this guide for?

This guide is intended for use by:

- New customers installing the Clearswift Secure Exchange Gateway for the first time.
- Existing customers upgrading from an earlier version 4 release of the Clearswift Secure Exchange Gateway to version 5.1.0.
- Existing customers upgrading from the version 5.0.0 release of the Clearswift Secure Exchange Gateway to version 5.1.0.

2. Before installing

This section outlines prerequisites and considerations you need to make before installing the Clearswift Secure Exchange Gateway. The Gateway runs on 64 bit Red Hat Enterprise Linux (RHEL 7.8). 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 the Clearswift Secure Exchange Gateway using one 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 7.8 or above and the Clearswift software.	Installing from the ISO image

Installation process	Description	Where to start
Public Cloud (AWS, Azure or customer supplied OS)	Applies to users installing the product on an existing RHEL 7.8 or above platform.	Appendix A: Software Install Process
Packaged Hardware Platform	Applies to users deploying the product using pre-installed hardware supplied by Clearswift.	Configuring the Gateway

2.2 Obtaining the software

You can obtain the Clearswift Secure Exchange Gateway software from:

- The Clearswift download area where you can download the Clearswift Secure Exchange Gateway ISO image.
- The Clearswift support portal where you can download the Interceptor software.
- Clearswift, with your pre-installed hardware.

2.3 Prerequisites

Before installing, you should check that you have the following:

2.3.1 Hardware requirements

Your computer or virtual machine requires a minimum of 6 GB RAM and a 60 GB hard drive for use in testing and demonstration environments.

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

For a production environment, Clearswift recommends the following based on your storage and processing requirements where your Gateway is configured so that your policy has:

- 1 Anti-Virus Scanner
- Optical Character Recognition disabled

Type Email	Estimated Throughput	CPU Cores/vCPU	RAM (GB)	Disk (GB)	Raid
Physical - Low Spec	Under 20,000 msgs/hour	2	16	200+	Optional
Physical - High Spec	75,000 msgs/hour	4	16	300+	Yes
Virtual - Low Spec	Under 20,000 msgs/hour	2	10	200+	Optional

Type Email	Estimated Throughput	CPU Cores/vCPU	RAM (GB)	Disk (GB)	Raid
Virtual - High Spec	75,000 msgs/hour	4	16	300+	Yes

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

2.3.2 Installation media

Please ensure you are using the correct version of the ISO image:

- EXCHANGE-5.1.0.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.

2.3.3 Browser support

The Clearswift Secure Exchange 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)

2.3.4 Clearswift SXG Interceptor prerequisites

To install the Clearswift SXG Interceptor, you must have the following:

- Windows 2008 R2 with SP1
- Exchange Server 2013 or Exchange Server 2016
- Microsoft Active Directory Lightweight Directory Services (AD LDS)

AD LDS is only required if the SXG Configuration Store component is selected during install. The SXG Configuration Store component is selected by default during installation of the Clearswift SXG Interceptor. However installation of the SXG Configuration Store component is only required during installation of the Clearswift SXG Interceptor on the first server in your organization.

- Microsoft .Net 3.5
- PowerShell 2.0

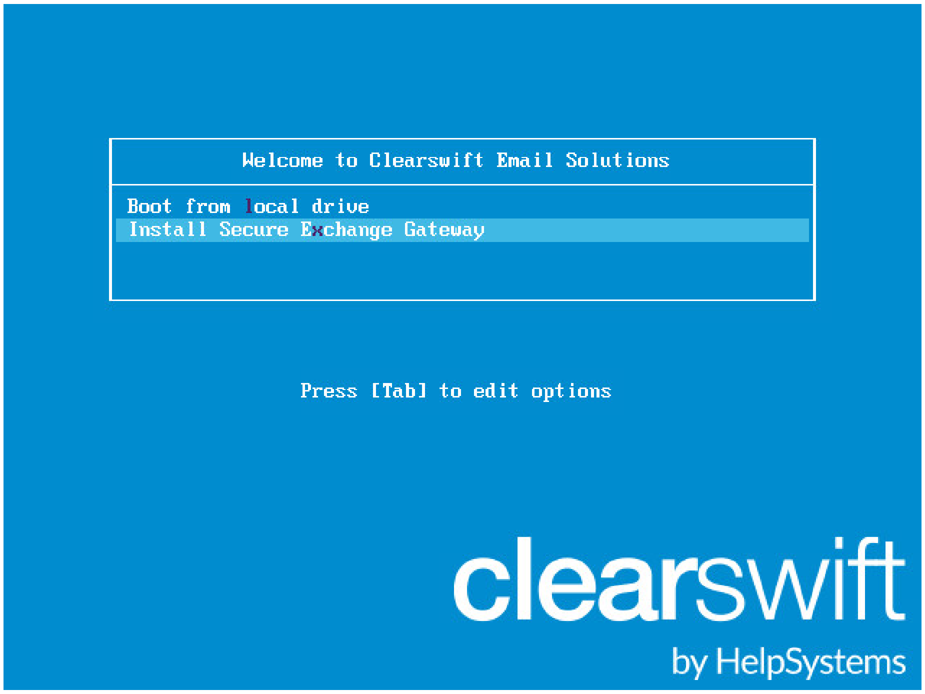
3. Installing the Clearswift Secure Exchange Gateway

You can install the Clearswift Secure Exchange Gateway software from the ISO image that you downloaded from the Clearswift download area.

3.1 Installing Red Hat 7.8 and 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.


Welcome to Clearswift Email Solutions
Boot from local drive
Install Secure Exchange Gateway
clearswift
by HelpSystems

Press [Tab] to edit options

2. Use the arrow keys or keyboard shortcuts to select **Install Secure Exchange 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.

> We *strongly recommend* configuring each network card with a static IPv4 network address.

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

> Warning! 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 Starting 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 is required because post-installation you are ***strongly advised*** to disable the root user account as a security precaution.
    - This can also be done post-installation via the Red Hat Cockpit application.
    - It is good practice to create a backup administrator user in case the primary administrator password is lost.

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

3.3 Configuring the Gateway

On restart, you will need to complete the Clearswift Secure Exchange Gateway Installation wizard.

1. Open a supported Web browser and navigate to the Gateway IP address:

   https://<ip-address>/Appliance

2. The 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 Gateway Installation Wizard. The wizard requires access to the installation media to complete the setup of your 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 Clearswift Secure Exchange Gateway. We recommend visiting the First Steps topic in the online help when the Gateway interface is accessible.

3.4 Creating Administrator Accounts

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

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

This can be achieved using the Red Hat Cockpit application.

1. Enter the following URL into a supported web browser to load the Cockpit Administration User Interface.

   https://<ip-address>:9090

2. Log in to Cockpit using the credentials created during the Red Hat installation, ensuring **Re-use my password for privileged tasks** is checked.

   > On first login you will be asked to change the user password.

Once this has been done you should log out and then log back in, otherwise you will not have full administrator privileges.

3. Select **Accounts** and click **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**. Then select 'Never lock account' and click **Change**.
   - Select **Never expire password** or the **date** on which the password will expire. Then click **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 'Re-use my password for privileged tasks' setting.
6. Select Accounts and click the root user.
   - Select the **Lock Account** setting 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 Configuring 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 Gateway releases.

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

- Switching from offline to online repositories gives access to Red Hat security fixes, normally within 24 hours of their publication. We recommend this for most installations.
- However, you should only do this if you intend to also use online repositories for future Clearswift product upgrades.

Online repositories can be enabled by following the steps below:

Be aware that enabling online repositories is an irreversible action.

1. Enter the Cockpit URL into a supported web browser to load the Cockpit Administration User Interface. Then login using the administrator credentials, ensuring that you have selected the **Re-use my password for privileged tasks** setting.
2. Select Clearswift and then under **Product Actions**, click **Enable** in the Enable online repositories setting.

4. Installing your Clearswift SXG Interceptor

Depending on your organization's requirement and infrastructure you have the following options:

- Single Microsoft Exchange Server, single Clearswift SXG Interceptor, and single Gateway
- Single Microsoft Exchange Server, single Clearswift SXG Interceptor, and multiple Gateways
- Multiple Microsoft Exchange Servers, multiple SXG Interceptors, and multiple Gateways

Sections 4.1 to 4.6 in this guide assume a Single Microsoft Exchange Server, single Clearswift SXG Interceptor, and single Gateway configuration.

For installing additional SXG Interceptors, please see section 4.7 Installing Multiple SXG Interceptors.

Before you install your Clearswift SXG Interceptor, the following steps need to be completed on the Exchange Gateway and Exchange Server:

4.1 Configure the Secure Exchange Gateway

1. Install and set up the Secure Exchange Gateway as described in section 3 of this installation guide.
2. Create a DNS entry for the Exchange Gateway.
3. Add your Exchange Server to the **Exchange Servers** page on the Secure Exchange Gateway.

   For information on how to do this, see *Configure Gateway to Exchange Server communication* in the Exchange Gateway online Help.
4. Make a note of the Exchange Server's **Client ID**.

4.2 Configure Active Directory

You need to create a Universal security group and create a user that will be used to access the Configuration store.

1. Create the universal security group.
   a. From **Active Directory Users and Computers**, create a group called ***Clearswift SXG Administrators*** in the root domain of the forest. Ensure **Group scope** is set to **Universal**.
2. Create the user to be used to access the Configuration Store.
   a. From **Active Directory Users and Computers**, create a user in the root domain of the forest. Select the **Password never expires** check box.
3. Add the user to the ***Clearswift SXG Administrators*** group.

4. Add the user that will be performing the Interceptor install to the ***Clearswift SXG Administrators*** group.
5. Add any users that will be using the Clearswift SXG Interceptor Powershell cmdlets to the ***Clearswift SXG Administrators*** group.
6. Log out and then log in to ensure permissions are activated.

4.3 Install your Clearswift SXG Interceptor

1. Go to https://community.helpsystems.com/products-and-downloads/downloads/
2. Download the Clearswift SXG Interceptor installer to a location on your Microsoft Exchange server.
3. Log on to your Microsoft Exchange server using an account that is a member of the Clearswift SXG Administrators group.
4. Using Windows Explorer, locate the downloaded Clearswift SXG Interceptor installer and then run it.
5. Follow the instructions in the setup wizard.

   You will find extra information about the wizard pages in the following table:

Wizard page	Extra information
Feature Selection	Select the following options for a first Interceptor install in a new deployment: ▪ Clearswift SXG Interceptor ▪ Clearswift SXG Interceptor Configuration Store ▪ Clearswift SXG Management Shell Note: Any features that you choose not to install are offered when the installer is run again. Clear the **New instance** check box if you do not want to install the configuration store on your Microsoft Exchange server. Note: The configuration store must be installed on another server before you can install the Interceptor without a configuration store.
Prerequisite Checks	Make sure that all your versions of Exchange, PowerShell, Microsoft.Net and Active Directory Lightweight Directory Services (AD LDS) are supported.
Installation Settings	If you are installing the Clearswift SXG Interceptor, you must provide the Exchange server's client ID. **Tip**: Copy and paste the client ID from the Exchange Server page on the Exchange Gateway. If you haven't got a client ID at this stage, you can set one after you have installed the Clearswift SXG Interceptor.

Wizard page	Extra information
	For more information, see the *Work with Client IDs* section of Configure Gateway to Exchange Server communication in the Exchange Gateway online help.
Microsoft AD LDS Credentials	Provide the user name that you created to access the configuration store in the format *DOMAIN\username*. The account should have rights to install, and then access, the new instance of the Clearswift SXG Interceptor configuration store.

4.4 Complete the SXG Interceptor installation

You need to perform the following tasks, as a minimum, to complete the installation:

1. Add an SXG Gateway
2. Enable the SXG Gateway
3. Enable the Clearswift SXG Interceptor

Optionally, after these steps, you can:

- Add interception rules
- Enable monitor mode
- Configure performance counters
- Check that the installation is valid

This section describes the mandatory tasks.

To add an SXG Gateway, you use the **Add-SXGGateway** cmdlet. To do this:

1. Click **Start** > **All Programs** > **Clearswift SXG Interceptor** > **Clearswift SXG Interceptor Management Shell**.

> If using Windows Server 2012, go to the start screen and click the **Clearswift SXG Interceptor Management Shell** icon.

2. Add the Gateway. From the command line type the following:

```
Add-SXGGateway [[-Identity] <GatewayIdentity>] [<CommonParameters>]]
```

where:

- *<GatewayIdentity>* is the Fully Qualified Domain Name (FQDN) of the SXG you want to add

To find the FQDN, from the SXG UI click **System** > **Ethernet Settings**.

- *<CommonParameters>* is a list of optional common parameters, for example, verbose, debug.

Detailed cmdlet help is available from the **Clearswift SXG Interceptor Management Shell** and each cmdlet has extended help options. For example, to see examples for *Add-SXGGateway*, type the following at the prompt:

```
get-help Add-SXGGateway -examples
```

For further technical information, type the following commands at the prompt:

```
get-help Add-SXGGateway -detailed
```

```
get-help Add-SXGGateway -full
```

To see a list of cmdlets, type the following at the prompt:

```
get-command -module SXGInterceptor
```

3. Enable the Gateway. From the command line type the following:

```
Set-SXGGateway [[-Identity] <GatewayIdentity>] -Enabled
$true
```

- *<GatewayIdentity>* is the FQDN of the SXG you want to enable

4. Enable the Interceptor. From the command line type the following:

```
Set-SXGInterceptor [[-Identity] <InterceptorIdentity>] -
Enabled $true
```

- *<InterceptorIdentity>* is the FQDN of the server where the Clearswift SXG Interceptor is installed

ⓘ By default, Interceptors will only use Exchange Gateways in the same peer group and in the same AD site. However, this behaviour can be manually overridden. For more information, see the *How do I Work with Automatic and Manual Site Assignment* section of Configure Gateway to Exchange Server communication in the Exchange Gateway online help.

For help including configuration tasks you need to perform on your Exchange Gateway, interception rule creation, and performance monitoring, see the Exchange Gateway online help.

4.5 Validate the Clearswift SXG Interceptor installation

You can validate the Clearswift SXG Interceptor installation by running the following commands from the **Clearswift SXG Interceptor Management Shell**:

```
Get-SXGSettings
```

Expected result: The AD LDS username, logging level and security protocol types should be displayed.

```
Get-SXGInterceptor
```

Expected result: Interceptor details should be displayed. Note that there will be no details if the first installation is a configuration store on a non-Exchange server.

```
Get-SXGInterceptionRules
```

Expected result: Default rules should be displayed.

```
Get-SXGGateway
```

Expected result: The reported sites should include the site Exchange is in.

4.6 Test your Clearswift SXG Interceptor

1. On your Exchange Server computer, send a test email message using either Outlook or the Outlook Web App.
2. On your Exchange Gateway, go to the **Home** page, and then view the **Recent Messages** area.
3. View the Clearswift SXG Interceptor log(s) located in C:\ProgramData\Clearswift\SXGInterceptor\logs
4. Using **Event Viewer**, view the **Applications** event log.

4.7 Installing Multiple SXG Interceptors

This section guides you through the process of installing second, and subsequent SXG Interceptors.

4.7.1 Prerequisite Checks

Make sure that all your versions of Exchange, PowerShell, Microsoft.Net and Active Directory Lightweight Directory Services (AD LDS) are supported.

4.7.2 Feature Selection

Select the following options for each new Interceptor install:

- Clearswift SXG Interceptor (Required)
- Clearswift SXG Interceptor Configuration Store (Optional but recommended)
- Clearswift SXG Management Shell (Required)

4.7.3 Installation Settings

You must provide the Exchange server's client ID.

> Copy and paste the client ID from the Exchange Server page on the Exchange Gateway.

4.7.4 Microsoft AD LDS Credentials

Provide the user name that you created to access the configuration store in the format: **DOMAIN\username**.

The account should have rights to install, and then access, the new instance of the Clearswift SXG Interceptor configuration store.

4.7.5 Installation

1. Download the Clearswift SXG Interceptor installer to a location on the next Microsoft Exchange server.
2. Log on to your Microsoft Exchange server using an account that is a member of the Clearswift SXG Administrators group.
3. Using Windows Explorer locate the downloaded Clearswift SXG Interceptor installer and then run it.
4. Follow the instructions in the setup wizard.

4.7.6 Upon completion

When installation has completed, do the following:

1. Click **Start** > **All Programs** > **Clearswift SXG Interceptor** > **Clearswift SXG Interceptor Management Shell**.

2. Check the Clearswift SXG Interceptor status by running the following command:

   ```
   Get-SXGInterceptor
   ```

3. If the Interceptor is disabled, enable it by running the following command:

   ```
   Set-SXGInterceptor -Identity <InterceptorIdentity> -Enabled
   $true
   ```

   Note: *<InterceptorIdentity>* is the FQDN of the server where the Clearswift SXG Interceptor is installed.

4. Send a test message through the Exchange server.
5. Confirm the second interceptor is communicating to the SXG Gateway by navigating to the Exchange servers page in the SXG Gateway UI and verifying the connectivity to the Exchange Server.

5. Upgrading From Gateway 4.x

ⓘ If you are installing the Clearswift Secure Exchange Gateway for the first time, please ignore this section.

5.1 Preparing to 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 Clearswift Secure Exchange Gateway software on one of these, refer to Appendix B: Resolving Upgrade Failures for further information.

5.3 Checking Prerequisites

4.11.2 is minimum version required to upgrade to Gateway 5.1.0.

You will also need to download a copy of the version 5.1.0 ISO to complete an upgrade from 4.11.2. See Prerequisites for more information.

To upgrade your Gateway to Gateway 5.x you need to do the following:

1. Using the Clearswift Server Console, upgrade your Gateway 4.x server to version 4.11.2 using the standard upgrade previously used to upgrade 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 7.8 and Gateway software if met.

- Please ensure you follow the upgrade instructions in the Secure Exchange Gateway 4.11.2 Installation Guide so that your Gateway is correctly configured before attempting to upgrade to version 5.1.0.

On completion of the 4.11.2 upgrade, you will be ready to upgrade to Red Hat 7.8 and Gateway 5.1.0.

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

```
sudo su
```

3. Check your Gateway v5.1.0 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:

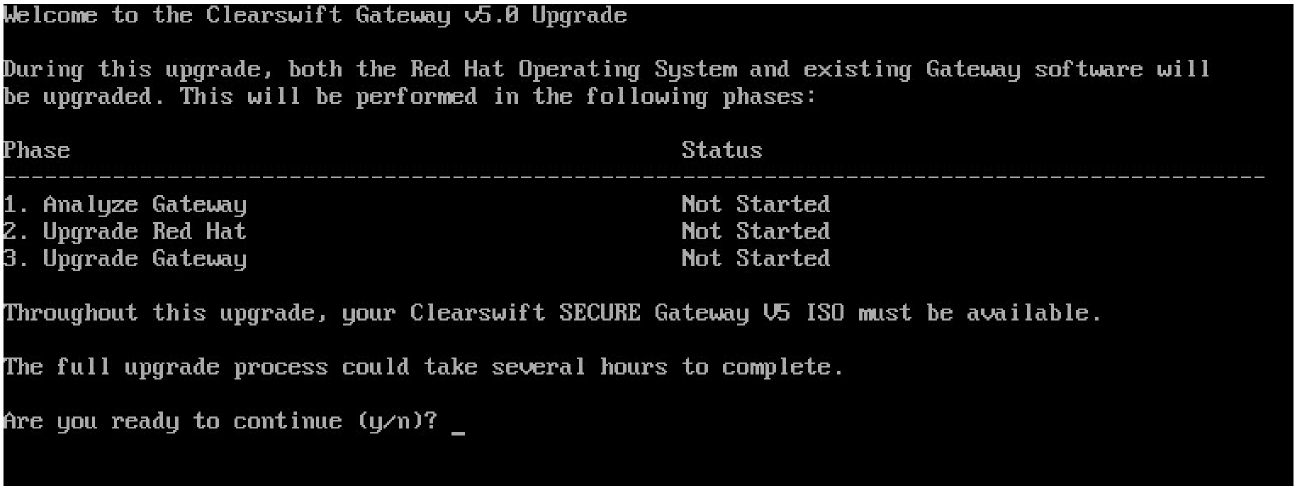
```
cs-gateway-v5-upgrade.sh
```

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 7.8

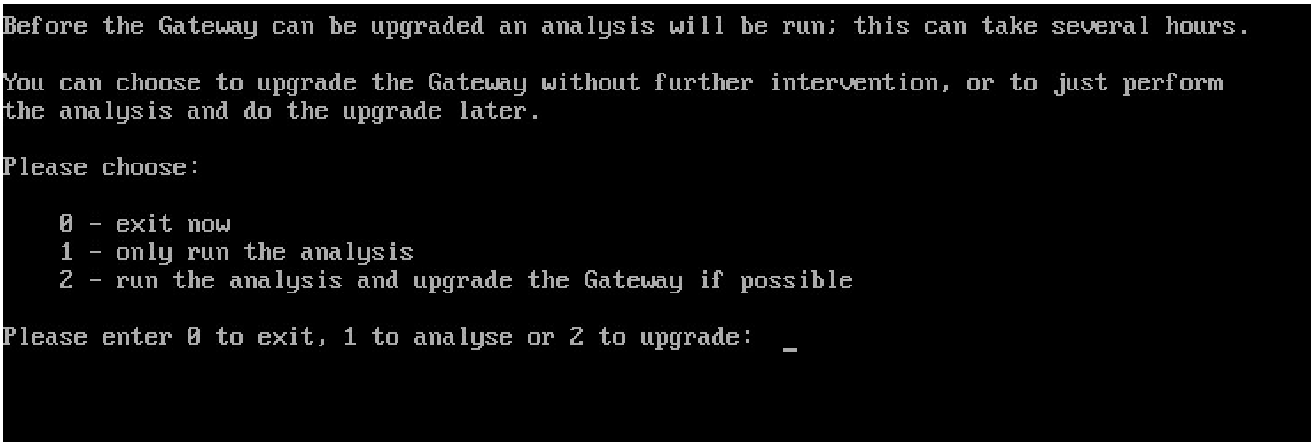
Assuming the pre-requisites are met, the following phases will be run to upgrade the software:

- **Upgrade Red Hat** will perform the migration of Red Hat 6 to Red Hat 7.8
- **Upgrade Gateway** will upgrade the 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. Please do not restart your 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 7.8.

In the event of your Gateway not meeting the necessary pre-requisities to be upgrade, please refer to Appendix B: Resolving Upgrade Failures.

5.4 Upgrading the Gateway

Follow the steps below to continue upgrading Red Hat 6 to 7.8.

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 the Red Hat Cockpit application and create new administrator account(s) that you will then use to administer the 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 the Gateway from a Gateway 4.x Terminal Session is no longer available in Gateway 5.0 onwards.

3. The upgrade of Red Hat 6 to 7.8 will now begin. The server will reboot midway through and then complete the upgrade during the server restart.

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 Gateway's Web UI once the upgrade is complete.

5.5 Post-Upgrade Actions

The Red Hat and 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 server initializes.

5.5.1 Create new Administrator Account(s)

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

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

See Creating Administration Accounts for further information on creating new accounts.

> The cs-admin user account previously used in Gateway 4.x is not supported. You must use a new Administrator Account instead.

5.5.2 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.

5.5.3 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.

5.5.4 Future Updates

You will be notified of future updates in the Gateway Administration UI and via the Red Hat Cockpit application.

1. Enter the following URL into a supported web browser to load the Cockpit Administration UI:

   https://<ip-address>:9090

2. Select 'Software Updates' and click **Check for Updates**.

See Configuring Update Repositories for instructions on how to enable Online Update Repositories if you would like to retrieve updates from those repositories.

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 Exchange Gateway from the Clearswift 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 Clearswift Technical Support if you need additional guidance on how to complete this step.

6. Upgrading From Gateway 5.x

If you are installing the Clearswift Secure Exchange Gateway for the first time, please ignore this section.

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

6.1 Upgrading From ISO

Use Cockpit to install the upgrade from the v5.1 ISO image.

6.1.1 Important Notes

You must make the v5.1 ISO image available to your Gateway, noting that in v5.1 there is an ISO image per product.

If you are using a DVD and if it doesn't mount automatically you may have to type the following at the command-line:

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

6.2 Upgrading From Online Repositories

Please follow the procedure detailed within the Future Updates section. Please see "Upgrading from Gateway 4.x - Future Updates" for more information.

6.2.1 Important Note

After the upgrade you will find that your upgrade mode has been reset to "offline". Navigate to the Clearswift section of Cockpit and select **Enable online repositories**.

7. Troubleshoot your Clearswift SXG Interceptor

The following can help you locate problems with your Exchange Interceptor installation.

7.1 Display information about the Interceptor

1. Open the **Clearswift SXG Interceptor Management Shell**.
2. Type the following:

```
Get-SXGInterceptor | Format-List
```

The following information is displayed with values applicable to your Interceptor:

```
Identity             : HUB1.example.com
InterceptorIdentity  : HUB1.example.com
State                : Active
Enabled              : True
ClientID             : 94bbc203-81a2-45be-a5ff-54c6a3dadad3
MonitorModeEnabled   : False
QueueLength          : 0
Version              : 4.10.0.n
```

> The State should read as Active if the SXG Interceptor is enabled and the Microsoft Exchange Transport Service has received a message.

7.2 Check that the Clearswift SXG Interceptor is installed as a transport agent

1. Open the **Clearswift SXG Interceptor Management Shell**.
2. Type the following:

```
Get-TransportAgent
```

The following information is displayed.

```
Identity                                                 Enabled
      Priority
--------                                                 -------
      --------
Transport Rule Agent                                     True
      1
```

```
Text Messaging Routing Agent                       True
      2
Text Messaging Delivery Agent                      True
      3
ClearswiftSXGInterceptor                           True
      4
```

7.3 Set the logging level

You can set the logging level by using the following command from the **Clearswift SXG Interceptor Management Shell**.

```
Set-SXGSettings -LogLevel [Off|Error|Warn|Info|Debug]
```

The logs are generated in the “C:\ProgramData\Clearswift\SXGInterceptor\logs” directory on the Exchange Server.

Appendix A: Software install process

The following steps describe how to install the Clearswift Secure Exchange Gateway on top of an existing Red Hat Enterprise Linux (RHEL) 7.8 Server (including a suitably configured AWS or Azure instance).

You should install Red Hat 7.8 as a **Minimal** server installation, with a separate /(root) and /var partition. The root partition should be 20GB (minimum) and /var should use a minimum of 60 GB for test environments and 200GB for production environments.

If you want to secure your Red Hat 7.8 Server to DISA STIG Compliance standards, you will need to apply this profile before you continue with the Gateway installation. See Appendix F for details.

Installing from Gateway ISO

To install the Clearswift Secure Exchange 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 Clearswift Secure Exchange 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 future, enter the following to install the required configuration files:

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

6. Install the required product using the following command:

```
yum install -y cs-sxg
```

If Step 6 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 Configuring the Gateway.

Installing from Clearswift Online Repositories

To install Clearswift Secure Exchange Gateway from repositories hosted online by Clearswift, you will need 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 the link 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/sxg/cs-rhel7-mirrors-21.04.00.rpm

curl -Of https://products.clearswift.net/rhel7/sxg/cs-sxg-repo-5.1.0.rpm
```

3. Download and install the Clearswift GPG public key:

```
rpm --import https://products.clearswift.net/it-pub.key
```

4. Verify the downloaded packages:

```
rpm --checksig --verbose cs-*.rpm
```

This will display the results below, where all checks respond with OK:

```
cs-sxg-repo-5.1.0.rpm:

 Header V4 RSA/SHA1 Signature, key ID 5522142c: OK
 Header SHA1 digest: OK (a39e783b63cd5c6d343123f0b9757b352c74f2bb)
 V4 RSA/SHA1 Signature, key ID 5522142c: OK
 MD5 digest: OK (ea4557f001ef99326b27f749c0d33447)
```

```
cs-rhel7-mirrors-21.04.00.rpm:

 Header V4 RSA/SHA1 signature, key ID 5522142c: OK
 Header SHA1 digest: OK (33a4f7494e105be9deae71984f33b9a565d55301)
 V4 RSA/SHA1 Signature, key ID 5522142c: OK
 MD5 digest: OK (6d3e2e1db3a2e3896736790deb29a43f)
```

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-sxg --enablerepo=cs-*,ext-cs-*
```

   This command temporarily enables access to the Clearswift online repositories and installs the Gateway.

> If Step 6 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 the Gateway.

Post installation considerations

1. All system administration actions should be performed using the Red Hat Cockpit application. Enter the following URL into a supported web browser to open Cockpit:

   https://<ip-address>:9090

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

2. If you want to secure your Gateway using the DISA STIG security profile, see Appendix F for further instructions.
3. The Firewall configuration will be controlled via the Gateway Administration User Interface. If SSH access is required you need to re-enable it through the Clearswift Secure Exchange Gateway user interface. See SSH Access in the Clearswift Secure Exchange Gateway online help for more information.
4. The crontab configuration is modified. Pre-existing root cronjobs might be lost, but you can re-add them.

Installing 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: Resolving upgrade failures

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

Gateway does not meet Red Hat 7.8 pre-requisites

If the upgrade failed because your Gateway did not meet the Red Hat pre-requisites for upgrading to Red Hat 7.8, you should review the analysis report below:

- /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.

Importing Gateway 4.x Backup to 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 Gateway 5.x server and then import a Gateway 4.x backup.

> Importing a Gateway 4.x backup does not automatically restore the peer group roles so they must be restored manually.

Restoring Peer Group Roles

Use the following to restore peer groups.

Using PMM

1. Open **System** > **PMM Settings** > **Portal Settings**.
2. Ensure the “Digest Generator” and “Portal” roles are each assigned to a peer.

> See Backup and Restore the system in the Clearswift Secure Exchange Gateway online help for more information.

Appendix C: USB installation media preparation

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

1. Download the Clearswift Secure Exchange Gateway software ISO image from the Clearswift download area.

   ⓘ 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. Clearswift recommends using Rufus Portable.

   ❗ Do not use the standard version of Rufus for this process. Please ensure it is the portable version.

   ⓘ Although you can use USB tools other than Rufus, the following USB tools will not work with the Clearswift Secure Exchange Gateway software ISO image:

   - YUMI
   - Universal USB Installer
   - Fedora liveusb-creator

   The below steps assume that you are using Rufus 3.11 Portable.

3. Run **rufus-3.11p.exe**.
4. Insert your USB media and select it from the **Device** drop-down menu.
5. Under **Boot Selection**, click the **SELECT** button to choose the Clearswift Secure Exchange Gateway 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 the Clearswift Secure Exchange 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	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 you are using PMM)
80	TCP	Out	Access to Clearswift product and Operating System updates at repo.clearswift.net and rh.repo.clearswift.net
80	TCP	Out	HTTP access to the Sophos, Avira, or Kaspersky 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** Kaspersky update servers: **kav-update-8-1.clearswift.net, kav-update-8-2.clearswift.net, kav-update-8-3.clearswift.net, kav-**

Port	Protocol	Direction	Required for
			update-8-4.clearswift.net, kav-update-8-5.clearswift.net, kav-update-8-6.clearswift.net
80	TCP	Out	HTTP access to the Gateway online help
80	TCP	Out	Access to the Service Availability List: 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 scannning the 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 access to the Clearswift Secure Exchange Gateway web interface and for communications between Peer Gateways
443	TCP	In/Out	Kaspersky KSN lookup. (While this is using port 443, the traffic is not standard HTTP/S. Do not try to route through an SSL proxy.) The KSN lookup servers are: **ksn1.kaspersky-labs.com, ksn2.kaspersky-labs.com, ksn3.kaspersky-labs.com, ksn4.kaspersky-labs.com**
443	TCP	Out	HTTPS access to the Clearswift Update Server for license management and handling Managed Lexical Expression Lists
443	TCP	In/Out	HTTPS Key Server Queries
445	TCP	Out	User authentication using NTLM (when using PMM in Full Mode)

Port	Protocol	Direction	Required for
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 the 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

Exchange Server Firewall Ports

The following table lists the ports you might need to open in Windows Firewall on your Exchange Server:

Port	Protocol	Direction	Required for
10443	TCP	Out	HTTPS access to the Clearswift Secure Exchange Gateway web service.
23953	TCP	In/Out	Communication with other SXG Interceptors.
23955	TCP	In/Out	LDAP access to SXG configuration store.

Appendix E: Password policy

The default password policy applied after 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

ⓘ Please 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 Gateway could be reduced.
>
> This is due to the increase in the level of auditing performed by the Red Hat audit service. Clearswift recommends that you carefully monitor performance before and after applying the profile, and assign additional hardware resources if required.

Installing via the Gateway ISO

If you have installed your Gateway using the ISO Image, the DISA STIG security profile is automatically applied for Red Hat 7.8. 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 7.8 Server both before and after the Gateway has been installed.

Upgrading a previous Gateway

If you upgraded from a previous version of the 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 Gateway Installation.

Applying Profile before the Gateway Installation

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

1. Open the terminal on your Red Hat 7.8 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 Gateway Installation

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

1. If you have not enabled online repositories, insert your Gateway ISO.
2. Open a supported Web browser and open Cockpit:

   https://<gateway-ip-address>:9090
3. Log in using your administrator account details and ticking the **Reuse my password for privileged tasks** option.
4. Click **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 the Gateway

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

1. Open a supported Web browser and open Cockpit:

   https://<gateway-ip-address>:9090
2. Log in using your administrator account details and ticking the Reuse my password for privileged tasks option.
3. Click Terminal.
4. Assume root user privileges using the following command

```
sudo su
```

5. Execute the following script

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

6. The report will be available from:

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

   > Customers wishing to validate their DISA STIG compliance can do so by contacting Clearswift customer support and requesting a compliance document.