clearswift

Clearswift SECURE Exchange Gateway

Installation & Getting Started Guide

Version 4.6.0

Document Revision 1.0

Copyright

Revision 1.0, April, 2017

Published by Clearswift Ltd.

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?

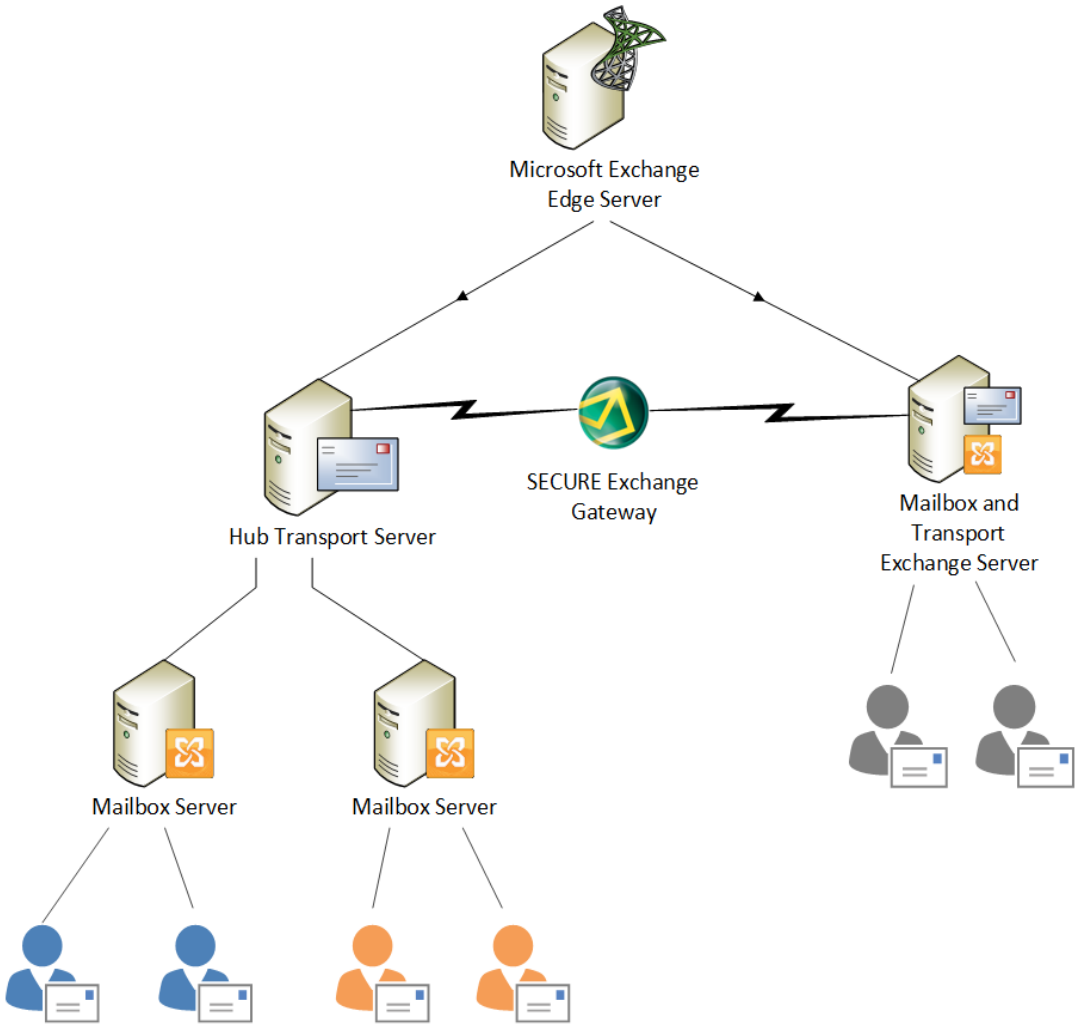
This guide is intended for use by:

- New customers installing the Clearswift SECURE Exchange Gateway for the first time.
- Existing customers upgrading from the most up to date version 3.8 release of the Clearswift SECURE Exchange Gateway to a 4.6.0 release.

If you are upgrading from an earlier version 4 release of the Clearswift SECURE Exchange Gateway, see the 4.6.0 Readme for guidance.

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 6.8). 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
Standard install process	Applies to users installing the product from an ISO image that contains both RHEL 6.8 and the	Installing from the ISO image

Installation process	Description	Where to start
	Clearswift software.	
Hardware install process	Applies to users deploying the product using pre-installed hardware supplied by Clearswift.	Running the Clearswift First Boot Console
Software install process (from ISO)	Applies to users installing the product on an existing RHEL 6.8 platform.	Appendix A: Software Install Process
Software install process (from online Clearswift repositories)	Applies to users installing the product on an existing RHEL 6.8 platform.	Appendix B: Software Install Process

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:

Hardware requirements

Your computer or virtual machine requires a minimum of 4GB RAM and a 60GB hard drive for use in testing and demonstration environments. Clearswift recommends a minimum of 200GB hard drive for use in a production environment based on your storage and processing requirements.

Message Volume	Processor	Number of Processors	Memory	Disk	Raid
Low (<20,000 per hour)	Dual Core	1	4GB	320GB+ SATA/SCSI	Optional

Message Volume	Processor	Number of Processors	Memory	Disk	Raid
Medium (<50,000 per hour)	Dual/Quad Core Xeon	1	4GB	320GB+ SATA/SCSI	Optional
High (<60,000 per hour)	Dual/Quad Core Xeon	1	6GB	2 x SAS 15k RPM	Yes (1)
Very High (>60,000 per hour)	Quad Core Xeon	2	6GB	Multiple SAS 15k RPM	Yes (1, 10)

Installation media

Please ensure you are using the correct version of the ISO image: EMAIL_460_160.iso.

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

- Copying the ISO image to DVD. Clearswift recommends using this option when installing the Clearswift SECURE Exchange Gateway software.
- Copying the ISO image to USB media. See Appendix B of this guide for instructions.
- Attaching the ISO image as a virtual DVD drive. This applies to virtual machines only.

Browser support

The Clearswift SECURE Exchange Gateway supports connections using TLS 1.2 ciphers and has been tested with the following browsers:

- Internet Explorer IE10 (Windows 7)
- Internet Explorer IE11 (Windows 7 , Windows 8)
- Mozilla Firefox 17, 24, 30, 36+

- Google Chrome 40+
- Microsoft Edge (Windows 10)

Clearswift SXG Interceptor prerequisites

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

- Windows 2008 SP2 and later
- Exchange 2007 SP3 or later
- 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 Online Clearswift Repository.

The installation process includes the following phases:

1. Combined installation of Red Hat Enterprise Linux 6.8 operating system and the Clearswift SECURE Exchange Gateway from the installation media.
2. Running the console-based *System Configuration* wizard to adjust default system values, including network configuration.
3. Enable access to the Clearswift online repositories containing the latest software updates.

Once the Gateway has been installed, you will need to complete the *Clearswift Installation Wizard*.

3.1 Installing the Clearswift SECURE Exchange Gateway

The following steps describe how to install the Clearswift SECURE Exchange Gateway.

Section 3.2 Installing from the ISO image only applies if you are performing a standard installation using the ISO image containing both RHEL 6.8 and the Clearswift software.

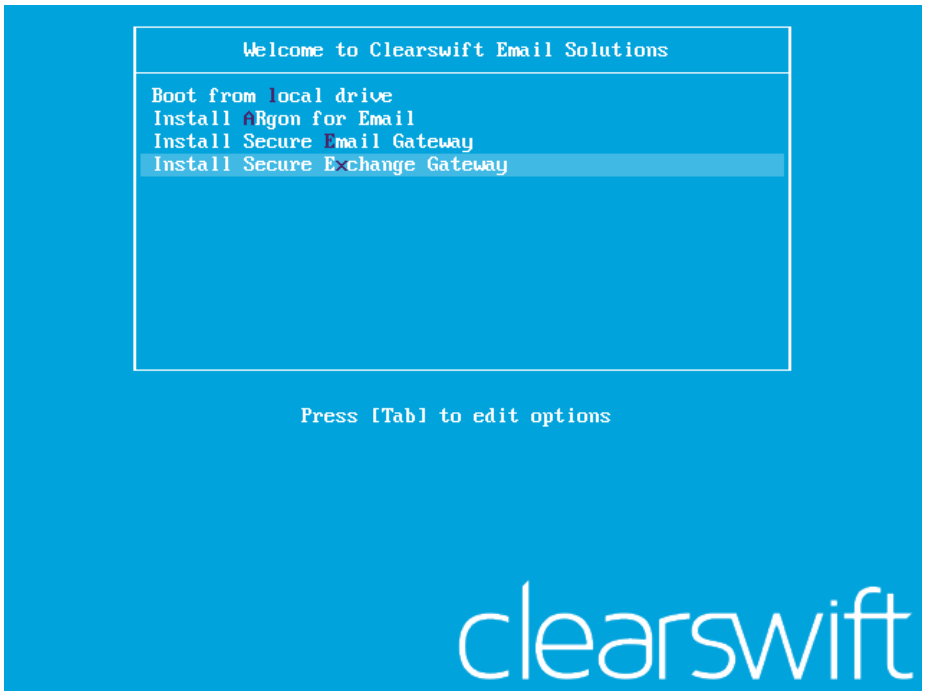
If you are performing the hardware install, go to Section 3.3 Running the Clearswift System Configuration wizard.

If you are installing onto an existing RHEL 6.8 server, use the instructions in Appendix A or Appendix B of this guide to perform the installation. Then refer to Section 3.3 Running the First Boot Console to complete the installation of the Clearswift SECURE Exchange Gateway.

3.2 Installing from the ISO image

1. Insert the media containing the ISO image into the drive and power on the server.

The *Welcome to Clearswift Email Solutions* 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 Exchange Gateway** from the menu. Press the **Enter** key to select the installation.

   The install process begins and runs automatically.

> The entire install process, including post-installation scripts, takes between 10-15 minutes to complete. After *Package Installation* completes, the install process displays the message "Running post-installation scripts" for a period of up to 5 minutes. When this message is on screen, the install process still runs in the background and you should not interrupt it. At the end of the install process, the system reboots automatically. The *Welcome to Clearswift Solutions* boot screen appears again and **Boot from local drive** triggers automatically after a timeout of 60 seconds.

3.3 Running the Clearswift First Boot Console

Complete the following steps in the *First Boot Console*:

1. Log in as cs-admin using the default credentials:
   - Login: **cs-admin**
   - Password: **password**

   The *First Boot Console* appears and you can start the configuration process.
2. Follow the on-screen instructions to select:
   - **Locale Configuration**
   - **Keyboard Configuration**
   - **Timezone Configuration**

   The Gateway derives its system time and locale settings from the selections made at this point. It is important that you set these correctly during installation as you cannot change system time and locale later.
3. On the **Network Configuration** page update the following settings:
   - System Hostname: Enter the new Hostname and press **Save**.
   - Network Adapters: Select a network adapter and press **Edit**. Press **IPv4 Addresses** and then **Edit** your selected IP address. After you have made your edits, press **Save**.
   - DNS Servers: Select a DNS entry and press **Edit**. Add **Search Domains** if required or leave blank.

     After you have made your edits, press **Save**.
4. Configure your repository settings on the **Repository Configuration** page.

   Clearswift online repositories are normally disabled by default after installation. This indicates updates are to be taken from the local media. However, if you have access to the Internet you might want to receive updates from the Clearswift online repositories by selecting **Online Mode**.
5. On the **cs-admin password** page enter a new password for your cs-admin

account. The complexity of this password depends on the password policy that is being enforced. The Clearswift password policy applies by default to standard installations from the ISO image. This policy requires you to set passwords that are a minimum of eight characters in length, do not resemble dictionary words (example: Pa55word), do not include sequences (example: 1234), and include at least one from three of the following:

- Uppercase letters
- Lowercase letters
- Digits
- Symbols

See Clearswift password policy requirements in the online help for more information, including examples. The online help also provides information on how to disable the password policy.

6. Apply your settings and confirm to reboot the server.
7. Following the reboot, open a browser and navigate to the Gateway IP address:

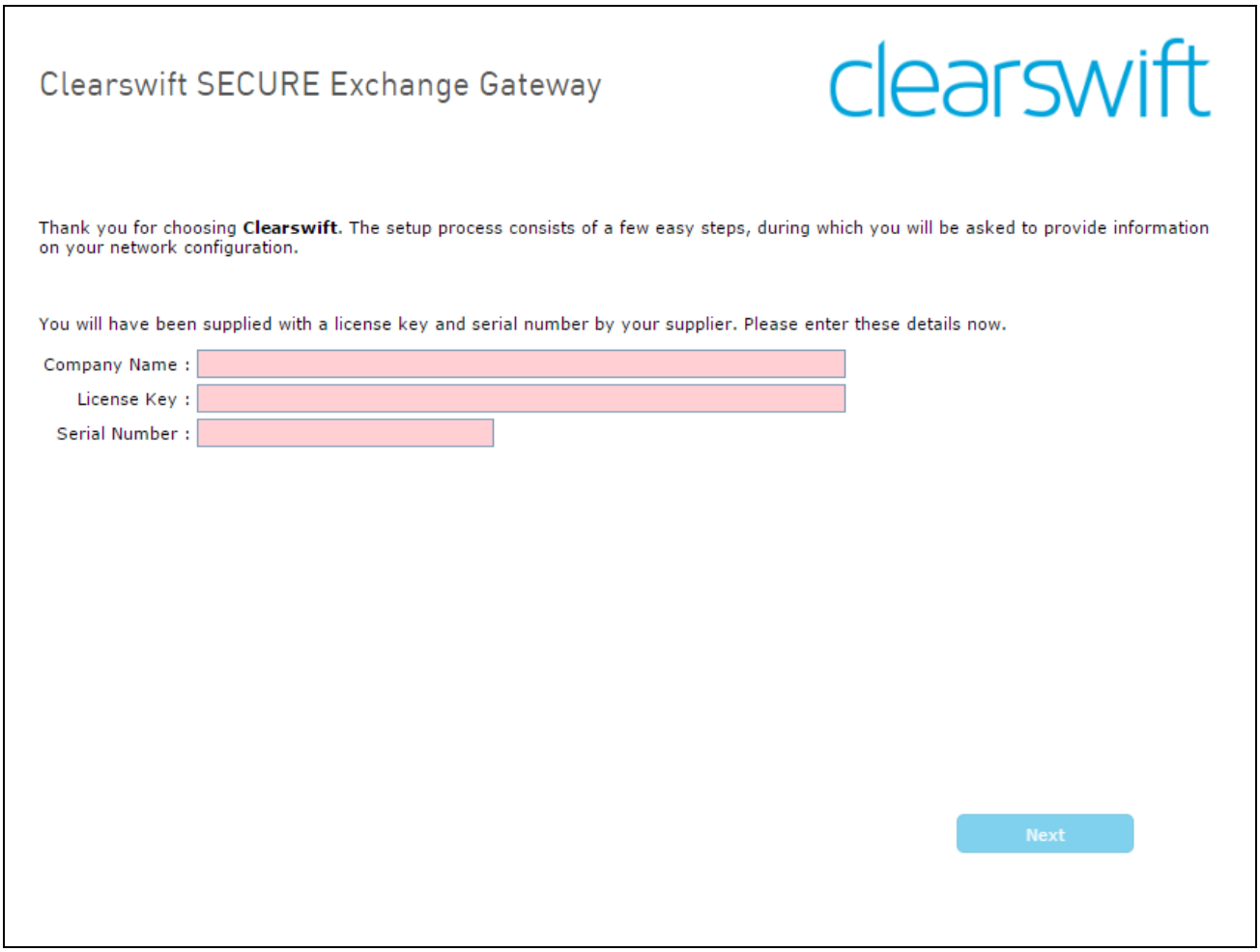
   https://<*ip-address*>/Appliance

   To check your IP address, log in to the console using the default credentials.

   Select **View System Status** and click **OK**.

   The *Clearswift SECURE Exchange Gateway* installation wizard is displayed.



The system might take around 5-10 minutes to apply the settings before you can use the Clearswift SECURE Exchange Gateway. We recommend visiting the First Steps topic in the online help when the Gateway interface is accessible.

If the Clearswift installation media has been ejected following the reboot, you **must** ensure that it is re-inserted *before* configuring the Clearswift Installation Wizard. The wizard requires access to the installation media to complete the setup of your Gateway.

Notes on using the Clearswift SECURE Exchange Gateway installation wizard

The network settings displayed by the wizard reflect the settings you created when configuring Red Hat Enterprise Linux. These settings are displayed as read-only.

We recommend configuring the wizard immediately after the install and *before* configuring any additional network adapters. However, if you need to reboot the machine before configuring the installation wizard, you should disable your firewall as root user when your reboot is complete. To disable your firewall, run the *service iptables stop* command. After you complete the wizard, the firewall starts again automatically.

Peering between v3 and v4 Clearswift Gateways

Due to security hardening on v4 Clearswift Gateways, we no longer provide support for the TLS v1.0 protocol for peering. Only TLS v1.2 is supported.

If you wish to peer v3 Gateways (for example, using PMM or Web Gateway Reporter) with your v4 Gateway, you must **re-enable TLS v1.0** on the 4.6.0 Gateway and **update the ciphers**.

If you are already running PMM on a v4 Gateway, you do not need to follow this procedure.

These instructions should be applied *after* installing the 4.6.0 Gateway, and after configuring the Gateway using the *Clearswift Installation Wizard*.

3.3.1 How to re-enable TLS v1.0 on the 4.6.0 Gateway and update ciphers:

1. Search for the **sslEnabledProtocols** attribute in the following files:

   ```
   /opt/tomcat/conf/
   server-bind.xml
   server-bind2.xml
   ```

2. Change the value of each protocol from 'TLSv1.2' to 'TLSv1,TLSv1.2'.

   There are two instances in server-bind2.xml.

3. Search for the **ciphers** attribute in the same files:

   ```
   /opt/tomcat/conf/
   server-bind.xml
   server-bind2.xml
   ```

4. Add 'TLS_RSA_WITH_AES_256_CBC_SHA' to the end of the comma separated list in each file.

   There are two instances in server-bind2.xml.

5. Restart the UI using the following command:

   ```
   cs-servicecontrol restart tomcat
   ```

3.4 Enabling or disabling access to the Clearswift online repositories

In Clearswift First Boot Console, you selected updates to be applied from either the online Clearswift repositories or your (offline) local media.

Clearswift online repositories are normally disabled by default after installation. This indicates updates are to be taken from the local media. However, if you have access to the Internet you might want to receive updates from the Clearswift online repositories by selecting **Online Mode**.

If you are using Microsoft Azure, you should note that the use of online repositories will download updates to your system and you will be charged by Microsoft for this download.

You can change the source for the online repositories later, if required. To do this:

Click **Configure System** > **View and Apply Software Updates** > **Enable/Disable use of 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.

Switching *from online to offline* is not supported and could lead to updating issues in the future.

To be confident that your system is up-to-date, you must apply system or product upgrades using Server Console. If you attempt to upgrade using the command line, it will report 'no updates available'.

---

4. Installing your Clearswift SXG Interceptor

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

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

The steps in the guide assume a Single Microsoft Exchange Server, single SXG Interceptor, and single Gateway configuration.

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

4.1 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 Exchange Server

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 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://www.clearswift.com/support/portals

2. Download the 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 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.

Wizard page	Extra information
	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 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 SXG Interceptor. 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 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 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 SXG Interceptor is installed

Interceptors can only use Exchange Gateways in the same peer group and in the same AD site.

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 SXG Interceptor installation

You can validate the 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 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 SXG Interceptor log(s) located in C:\ProgramData\Clearswift\SXGInterceptor\logs
4. Using **Event Viewer**, view the **Applications** event log.

5. Upgrading from version 3.8 of the Clearswift SECURE Exchange Gateway

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

If you are installing version 4.6.0 from an earlier version 3 Clearswift SECURE Exchange Gateway, please ensure your Gateway is fully upgraded to the latest 3.8 release and use the following instructions.

This section describes how to import your policy configuration and system settings from version 3.8 of the Clearswift SECURE Exchange Gateway to version 4.6.0. You should perform the backup steps *before* installing Clearswift SECURE Exchange Gateway 4.6.0.

Migrating from a V3 Gateway does not preserve network settings such as static hosts, static routes and DNS settings. Use the Server Console to re-apply your network settings when you have upgraded your Gateway. If you are using Client Integrated Authentication, you will also need to join the domain after migrating your Gateway.

5.1 Back up your original system

The system backup on an FTP server includes only the most recently applied configuration. If you require an earlier policy configuration along with quarantined messages, audit and tracking data and logs, you should first restore from the system backup and then restore the .bk file to your new Gateway, when installed.

1. Apply your configuration. This ensures that you are migrating the most up-to-date version.
2. Using your existing Gateway system, navigate to the **System Center** > **Backup & Restore** page.
3. Perform a System Backup using the **Backup System Now** option in the task panel.

We strongly recommend that you backup all available System Areas.

We recommend that you use system backups for a means of disaster recovery and for when planning to upgrade your system. Do not use them for any other purpose, for example, as a method of cloning Gateways when creating a peer group. For purposes other than disaster recovery and system upgrades you should use Configuration Backup and Restore.

5.2 Install the 4.6.0 Gateway

Follow the steps in section 3 of this installation guide to install the Clearswift SECURE Exchange Gateway.

When you have installed the Clearswift SECURE Exchange Gateway, you need to configure access to the Clearswift online repositories containing the latest software updates. See Enabling access to the Clearswift online repositories for more information.

Do not add 4.6.0 Gateways to the configuration until the Interceptors have been fully installed and upgraded.

We recommend installing a minimum of two Exchange Gateways (SXG) for each Active Directory site containing Exchange servers. The SXG Interceptor uses the IP address of the Gateway to define which AD site the Gateway is in.

4.6.0 Exchange Gateways must be peered, in order to maximize the flow of information between SXGs and Exchange Servers, and to share the Client IDs used by the SXG Interceptors.

5.3 Restore the system backup

1. Using the new, installed Gateway, navigate to the **System Center** > **Backup & Restore** page.
2. Select **Restore System** using the option in the task panel. Enter the FTP settings and click **Connect**.

The system restore includes all the areas you selected when you created your back-up, potentially including configurations and audit logs. The Gateway reboots after the system restore is complete.

6. Upgrading from version 3.8 of the Clearswift SECURE Exchange Gateway

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

If you are installing version 4.6.0 from an earlier version 3 Clearswift SECURE Exchange Gateway, please ensure your Gateway is fully upgraded to the latest 3.8 release and use the following instructions.

This section describes how to import your policy configuration and system settings from version 3.8 of the Clearswift SECURE Exchange Gateway to version 4.6.0. You should perform the backup steps *before* installing Clearswift SECURE Exchange Gateway 4.6.0.

Migrating from a V3 Gateway does not preserve network settings such as static hosts, static routes and DNS settings. Use the Server Console to re-apply your network settings when you have upgraded your Gateway. If you are using Client Integrated Authentication, you will also need to join the domain after migrating your Gateway.

6.1 Overview of the Upgrade Process

The following procedure is recommended as an upgrade route for migrating from version 3.8 to 4.6.0 of the SECURE Exchange Gateway. As an in-place upgrade is not currently possible, we recommend following the steps to perform a 'swing-server' approach:

1. Back up your configurations on any existing 3.8 Exchange Gateways.
2. Upgrade Interceptors on all Exchange Servers in the domain forest.
3. Install your Clearswift 4.6.0 SECURE Exchange Gateways (SXG) following the steps in this install guide. We recommend that you peer multiple SXGs.
4. Restore the configuration from your 3.8 Gateway to the newly installed 4.6.0 Gateway. Add any existing Gateway peers to the 4.6.0 configuration, where necessary.

5. Use the Add-SXGGateway cmdlet in the SXG Management Shell on the Exchange Server to add the 4.6.0 Gateways. Enable the new Gateways using the Set-SXGGateway cmdlet and disable the old Gateways using the Set-SXGGateway cmdlet.
6. Ensure that any held messages on the 3.8 Gateway are either released, deleted, forwarded or restored to the 4.6.0 Gateway. It is not possible to deliver these messages after the 3.8 Gateway has been removed.
7. Remove the 3.8 Gateways using the Remove-SXGGateway cmdlet.

We strongly recommend that you first perform this upgrade process in a pre-production environment which matches your live environment as closely as possible.

6.2 Back up your original system

The system backup on an FTP server includes only the most recently applied configuration. If you require an earlier policy configuration along with quarantined messages, audit and tracking data and logs, you should first restore from the system backup and then restore the .bk file to your new Gateway, when installed.

1. Apply your configuration. This ensures that you are migrating the most up-to-date version.
2. Using your existing Gateway system, navigate to the **System Center** > **Backup & Restore** page.
3. Perform a System Backup using the **Backup System Now** option in the task panel.

We strongly recommend that you backup all available System Areas.

We recommend that you use system backups for a means of disaster recovery and for when planning to upgrade your system. Do not use them for any other purpose, for example, as a method of cloning

Gateways when creating a peer group. For purposes other than disaster recovery and system upgrades you should use Configuration Backup and Restore.

6.3 Upgrade SXG Interceptors

All Exchange Servers in the organization with the *Transport* role (Exchange 2007 or 2010) or *Mailbox* role (Exchange 2013 or 2016) should have an existing SXG Interceptor installed. If an Interceptor is not installed on all servers, the Exchange Gateway(s) might not be able to process all internal mail within your organization.

Existing Interceptors should be upgraded to 4.6.0 before any 4.6.0 SXG Gateways are configured to process mail.

1. Locate the Interceptor installer and run the installation, following the setup wizard as described in section 4 of this installation guide.
2. Enter the account details for the SXG service account when prompted.

You do not need to stop the Microsoft Exchange Transport Service (MSExchangeTransport) before installing the SXG Interceptor. However, this service will stop during the upgrade process. Any queued messages will be delivered when the service restarts on completion of the upgrade.

We recommend that you schedule your upgrade for an off-peak time. Restarting MSExchangeTransport typically takes a few minutes but can take longer if messages are queued.

6.3.1 Uninstalling and Reinstalling

If for some reason you uninstall and reinstall the SXG Interceptor instead of upgrading, or if you add additional Exchange Servers and install the Interceptor for the first time, SSL3 will not be configured by default.

Configure your SXG Interceptor to include the SSL3 protocol. This enables the Interceptor to communicate with your existing 3.8 Exchange Gateways.

1. Run the following cmdlet in the SXG Management Shell:

   Set-SXGSettings –SecurityProtocolTypes “tls12 tls11 tls ssl3”

2. Monitor your 3.8 SXG Gateway and new Interceptor to make sure your configuration is operating as expected.

View the version of the SXG Interceptor by running the Get-SXGInterceptor cmdlet and identify version properties. For example:

Get-SXGInterceptor | Select-Object identity,version

Get-SXGInterceptor | fl identity,version

Get-SXGInterceptor | ft identity,version

6.4 Install the 4.6.0 Gateway

Follow the steps in section 3 of this installation guide to install the Clearswift SECURE Exchange Gateway.

When you have installed the Clearswift SECURE Exchange Gateway, you need to configure access to the Clearswift online repositories containing the latest software updates. See Enabling access to the Clearswift online repositories for more information.

Do not add 4.6.0 Gateways to the configuration until the Interceptors have been fully installed and upgraded.

We recommend installing a minimum of two Exchange Gateways (SXG) for each Active Directory site containing Exchange servers. The SXG Interceptor uses the IP address of the Gateway to define which AD site the Gateway is in.

4.6.0 Exchange Gateways must be peered, in order to maximize the flow of information between SXGs and Exchange Servers, and to share the Client IDs used by the SXG Interceptors.

6.5 Prepare Exchange Environment

You can add Clearswift SECURE Exchange Gateways (SXG) to the Interceptor configuration on your Exchange Servers at any point. However, you should not *enable* your Gateways until you have configured them and they are ready to process messages.

6.5.1 To add an Exchange Gateway to your SXG Interceptor environment:

1. Add 4.6.0 Gateways to the SXG Configuration using the Add-SXGGateway cmdlet using the Clearswift SXG Management Shell:

   Add-SXGGateway sxg1.example.com

   Add-SXGGateway 192.168.2.10

2. If you are using host names rather than IP addresses, make sure host 'A' records for the new Gateways are added to the DNS.

Where applicable, SXGs should be assigned to sites manually (if default configuration of automatic site assignment is not available). The SXG Interceptor uses the IP address of the SXG to find a matching site, but this can be overridden using the following cmdlet:

Set-SXGGateway sxg1.example.com -AssignedSites Site2

Gateway 'sxg1' is assigned to 'Site2'.

6.6 Prepare your SECURE Exchange Gateway Environment

When you have installed and peered the 4.6.0 Exchange Gateways, you should restore the configuration from your 3.8 Gateway. This can be done either by restoring a saved configuration file or by restoring from an FTP system backup.

If you restore a saved configuration, you will only restore configuration items such as policy routes, lexical expressions and Exchange Server ClientIDs. Use a system backup to restore held messages, reporting data and system logs.

6.6.1 Restore the system backup

1. Using the new, installed Gateway, navigate to the **System Center** > **Backup & Restore** page.

2. Select **Restore System** using the option in the task panel. Enter the FTP settings and click **Connect**.

The system restore includes all the areas you selected when you created your back-up, potentially including configurations and audit logs. The Gateway reboots after the system restore is complete.

6.6.2 System Backup Restore

A system backup restore includes system areas in addition to the policy configuration. If you choose to restore a Gateway using a system backup, you should migrate on a server-by-server basis, ensuring that the old Gateway is disabled before the new Exchange Gateway starts to process messages.

Network configuration is not restored from the old Gateway. To configure your network settings, use the Gateway console. For more information, see Networking Configuration in the online help.

6.6.3 Configuration Restore

A configuration restore is appropriate if you want the old Exchange Gateway to process mail alongside the new Gateway. For more information, see About Configuration Backup and Restore in the online help.

6.6.4 Completing Configuration

Before applying the configuration, ensure that the configuration items have been restored correctly:

- Policy definition (routes, content rules)
- Policy references (email addresses, disposal actions, lexical expressions)
- File lists
- Exchange Server Client IDs

If your 3.8 Exchange Gateway configuration includes Exchange Servers defined using a FQDN, these will be converted to IP addresses in your 4.6.0 Gateway configuration. This is because version 4.6.0 of the Exchange Gateway does not allow you to enter Exchange Servers using a FQDN. The IP address in the 4.6.0 configuration will be the result of the DNS lookup at the time you added the Exchange Server to the 3.8 Gateway configuration.

- Informs
- PMM user information (where applicable)

If you are restoring PMM from a backup, some additional configuration is necessary to configure the PMM portal.

Apply the configuration.

6.6.5 Peering

After completing applying the configuration following the restore, we recommend peering the 4.6.0 Exchange Gateway with any remaining 3.8 Exchange Gateways in your environment during the migration. You are able to:

- View message queues on all Gateways
- Track messages between Exchange Gateways or any existing peered Clearswift SECURE Email Gateways (SEG)
- View, release, forward or delete any held messages
- Access reports across both versions
- Share image data such as blacklisted or whitelisted images
- Access PMM data (where applicable)

Following the latest RHEL update, you are no longer able to peer a version 4 Gateway with a version 3 Gateway. For further details on this issue, including a fix, see "Unable to peer a version 3 Gateway with a version 4 Gateway following RHEL update" in the list of Known Issues in the Clearswift SECURE Exchange Gateway online help.

Each remaining Exchange Gateway must be operating at version 3.8.8 or later.

You cannot apply configuration between Gateways operating at different versions.

When peering Gateways, you might encounter compatibility warnings when attempting to apply configuration.

6.7 Enable your 4.6.0 Gateway

If you have upgraded the SXG Interceptors and restored configuration to your 4.6.0 SECURE Exchange Gateway, you can enable the 4.6.0 Gateway to process messages.

This enables the Gateway to receive mail from all the Interceptors in the AD site which match your new SXG IP address configuration.

6.7.1 To enable 4.6.0 Exchange Gateway

Run the Set-SXGGateway cmdlet in the SXG Management Shell. For example,

- Set-SXGGateway sxg1.example.com –Enabled $true

Enable the first 4.6.0 SXG and allow for a test period before phasing the deployment across your configuration.

6.7.2 To disable 3.8 Exchange Gateway

If you are phasing your deployment of 4.6.0 SXGs you can disable each 3.8 SXG using the following cmdlet after each corresponding 4.6.0 SXG is enabled:

- Set-SXGGateway sxg38.example.com –Enabled $false

Messages can still be processed while a Gateway is disabled, provided it is peered with a 4.6.0 Gateway. When removed, this is no longer possible.

Release, deliver or forward any held messages before *removing* the 3.8 SXG

6.8 Remove 3.8 Gateways

After testing, stabilization and monitoring of your Gateways, you should remove the 3.8 SXGs from your configuration.

Ensure no messages are held on the Gateway you want to remove.

6.8.1 To remove the 3.8 SXG Gateway

Run the following cmdlet:

- Remove-SXGGateway sxg38.example.com

6.8.2 Disable SSL3 on SXG Interceptors

When you have removed all your 3.8 Exchange Gateways, run the following cmdlet locally for each interceptor:

- Set-SXGSettings -SecurityProtocolTypes "tls12 tls11 tls"

7. Upgrading from an earlier version 4 release to version 4.6.0

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

Perform the following steps to download and apply software updates when you upgrade to Clearswift SECURE Exchange Gateway4.6.0.

Open an SSH session and access the Clearswift Server Console. Log in using your cs-admin access credentials.

Online or Offline mode?

Offline mode is designed for installations that operate in a closed environment, disconnected from the Internet. Unless this is a specific requirement for your system, you should install the Clearswift SECURE Exchange Gateway in online mode.

To perform an offline upgrade you require a copy of the latest release ISO mounted to suitable media (DVD/USB). Please contact Clearswift Technical Support if you need additional guidance on how to complete this step.

If you have online repositories enabled, updates will be downloaded overnight (automatically). You can apply them immediately. You can also use the **Check for New Updates** button if you believe that there has been a recent security fix issued.

1. Apply software updates:

   a. From the Clearswift Server Console main menu, select:

      Configure System > **View and Apply Software Updates** > **Apply Updates** > **OK**

   b. Confirm that you want to apply the updates by selecting **Yes**.

      All downloaded updates will now be installed. This process can take several minutes. A rolling progress log will be displayed. When the *Operation Complete* message appears, select **Done** to complete the install process.

At the end of the upgrade process the system might prompt you to either reboot or prompt you to log out. Follow the instructions on-screen.

Gateway services will restart automatically in either case.

8. Troubleshoot your SXG Interceptor

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

8.1 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               : Inactive
Enabled             : True
ClientID            : 94bbc203-81a2-45be-a5ff-54c6a3dadad3
MonitorModeEnabled  : False
QueueLength         : 0
Version             : 4.5.0.n
```

8.2 Check that the 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
```

8.3 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]
```

Appendix A: Software install process (from disc)

The following steps describe how to install the Clearswift SECURE Exchange Gateway on top of an existing Red Hat Enterprise Linux (RHEL) 6.8 Server (including a suitably configured AWS or Azure instance) using the ISO image.

You should install RHEL 6.8 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 60GB for test environments and 200GB for production environments.

To install the Clearswift SECURE Exchange Gateway:

1. Assume root role at the command line.
2. Insert the media containing the ISO image and mount it onto /media/os:

   ```
   mkdir -p /media/os
   ```

   ```
   mount /dev/cdrom /media/os
   ```

3. Manually install the cs-email-repo-conf package. The cs-email-repo-conf package configures your system to be ready for you to install the Clearswift SECURE Exchange Gateway:

   ```
   rpm -ivh /media/os/cs-repo/Packages/cs-email-repo-conf-*
   ```

4. Forcibly remove postfix, rsyslog and samba V3:

   ```
   yum -y remove postfix rsyslog samba-common
   ```

5. Install the required product using the following command:

   ```
   yum install -y cs-sxg --enablerepo=cs-*
   ```

   This command enables access to external repositories and ensures that only Clearswift repositories are subsequently used to install the Gateway.

   If Step 5 fails due to additional conflicts, you might need to remove additional packages during Step 4.

6. Log out completely, and log back in as cs-admin. Refer to Running the First Boot Console to continue.

Post installation considerations

After completing the software install process, the install process might have modified the following parts of your system:

1. Firewall configuration is now under Gateway control. If SSH access is required you need to re-enable it through the Clearswift SECURE Exchange Gateway user interface. See Configuring SSH Access in the Clearswift SECURE Exchange Gateway online help for more information.
2. All network configuration is now under Server Console control. 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.
3. crontab configuration is modified. Pre-existing root cronjobs might be lost, but you can re-add them.

After a software installation...

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 RedHat software.

From version 4.6 onwards, you will only be able to apply Clearswift-provided upgrades using the Clearswift Server Console. Server Console will ensure that only trusted Clearswift repositories are used during the upgrade process and will explicitly block any unintended updates from third-party repositories during the process.

Appendix B: Software install process (from Clearswift online repositories)

The following steps describe how to install the Clearswift SECURE Exchange Gateway on top of an existing Red Hat Enterprise Linux (RHEL) 6.8 Server (including

a suitably configured AWS or Azure instance) using the repositories hosted online by Clearswift. You will need Internet access to complete this installation.

You should install RHEL 6.8 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 60GB for test environments and 200GB for production environments.

To install the Clearswift SECURE Exchange Gateway:

1. Assume root role at the command line.
2. Manually install the cs-email-repo-conf package. The cs-email-repo-conf package configures your system to be ready for you to install theClearswift SECURE Exchange Gateway:

   ```
   rpm -ivh http://repo.clearswift.net/rhel6/gw/os/x86_
   64/Packages/cs-email-repo-conf-3.4.1-2526.x86_64.rpm
   ```

3. Forcibly remove postfix, rsyslog and samba V3:

   ```
   yum -y remove postfix rsyslog samba-common
   ```

4. Install the required product using the following command:

   ```
   yum install -y cs-sxg --enablerepo=cs-*
   ```

   This command enables access to external repositories and ensures that only Clearswift repositories are subsequently used to install the Gateway.

   If Step 5 fails due to additional conflicts, you might need to remove additional packages during Step 4.

5. Log out completely, and log back in as cs-admin. Refer to Running the First Boot Console to continue.

Post installation considerations

After completing the software install process, the install process might have modified the following parts of your system:

1. Firewall configuration is now under Gateway control. If SSH access is required you need to re-enable it through the Clearswift SECURE Exchange Gateway user interface. See Configuring SSH Access in the Clearswift SECURE Exchange Gateway online help for more information.
2. All network configuration is now under Server Console control. 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.
3. crontab configuration is modified. Pre-existing root cronjobs might be lost, but you can re-add them.

After a software installation...

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 RedHat software.

From version 4.6 onwards, you will only be able to apply Clearswift-provided upgrades using the Clearswift Server Console. Server Console will ensure that only trusted Clearswift repositories are used during the upgrade process and will explicitly block any unintended updates from third-party repositories during the process.

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.

Please ensure you are using the correct version of the ISO image: EMAIL_460_160.iso.

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 2.11 Portable.

3. Run **rufus-2.11p.exe**.
4. Insert your USB media and select it from the **Device** drop-down menu.
5. Under **Format Options**, select **Create a bootable disk using** and click the disk icon  to choose the Clearswift SECURE Exchange Gateway ISO you want to burn. Once Rufus scans the ISO, it fills in other options automatically.
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.