clearswift
RUAG Cyber Security

Clearswift SECURE Email Gateway
Installation & Getting Started Guide

Version 4.10.0

Document Revision 1.0

Copyright

Revision 1.0, April, 2019

Published by Clearswift Ltd.

Contents

1. About this guide

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

1.1 Who is this guide for?

This guide is intended for use by:

- New customers installing the Clearswift SECURE Email Gateway for the first time.
- Existing customers upgrading from an earlier version 4 release of the Clearswift SECURE Email Gateway to version 4.10.0.

2. Before installing

This section outlines prerequisites and considerations you need to make before installing the Clearswift SECURE Email Gateway. The Gateway runs on 64 bit Red Hat Enterprise Linux (RHEL 6.10). 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 Email 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 6.10 and the Clearswift software.	Installing from the ISO image
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 6.10 platform.	Appendix A: Software Install Process
Software install process (from online Clearswift repositories)	Applies to users installing the product on an existing RHEL 6.10 platform.	Appendix B: Software Install Process

2.2 Obtaining the software

You can obtain the Clearswift SECURE Email Gateway software from:

- The Clearswift download area where you can download the Clearswift SECURE Email Gateway ISO image.
- 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 6 GB RAM and a 60 GB 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.

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

Message Volume	Processor	Number of Processors	Memory	Disk	Raid
Low (<20,000 per hour)	Dual/Quad Core	1	8 GB	320GB+ SATA/SCSI	Optional
Medium (<50,000 per hour)	Quad/Hexa/Octa Core	1	8 GB	320GB+ SATA/SCSI	Optional
High (<60,000 per hour)	Quad/Hexa/Octa Core	2	8 GB	2 x SAS 15k RPM	Yes (1)
Very High (>60,000 per hour)	Quad/Hexa/Octa Core	2	8-16 GB	Multiple SAS 15k RPM	Yes (1, 10)

Installation media

Please ensure you are using the correct version of the ISO image: EMAIL_4100_4100.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 Email 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 Email 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 - latest

- Google Chrome - latest
- Microsoft Edge (Windows 10)

3. Installing the Clearswift SECURE Email Gateway

You can install the Clearswift SECURE Email 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 6.10 operating system and the Clearswift SECURE Email 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 Email Gateway

The following steps describe how to install the Clearswift SECURE Email 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 6.10 and the Clearswift software.

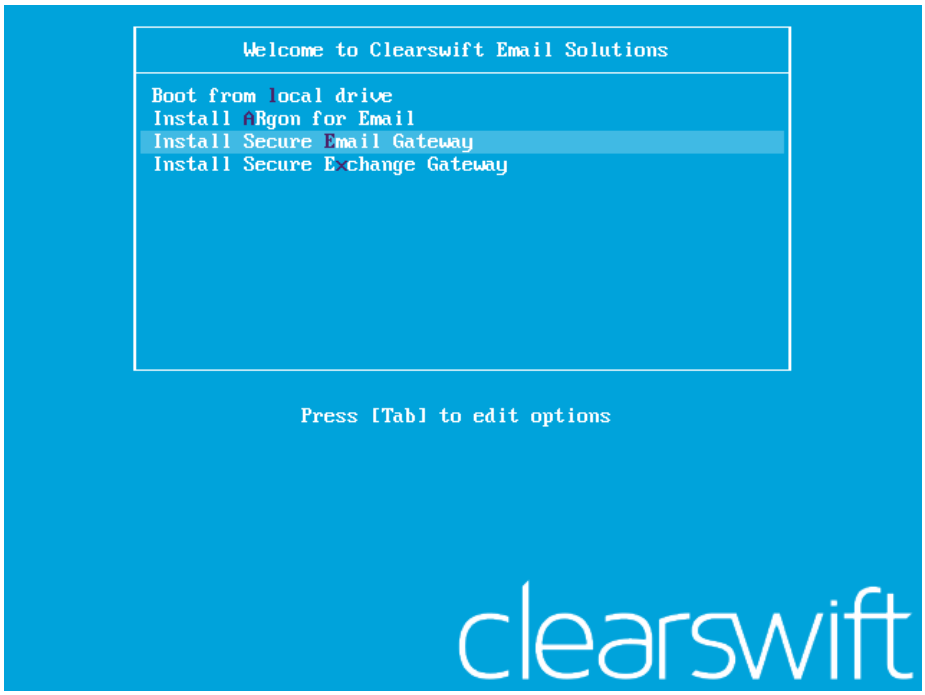
If you are performing the hardware install, go to Section 3.3 Running the Clearswift System Configuration wizard.

If you are installing onto an existing RHEL 6.10 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 Email 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 Email 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 Email 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**.

   > If you are installing the Clearswift SECURE Email Gateway on a hosted Microsoft Azure platform, we recommend reviewing the section on **How to change your network settings** in the Clearswift SECURE Email Gateway with Microsoft Azure Installation Guide.

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.

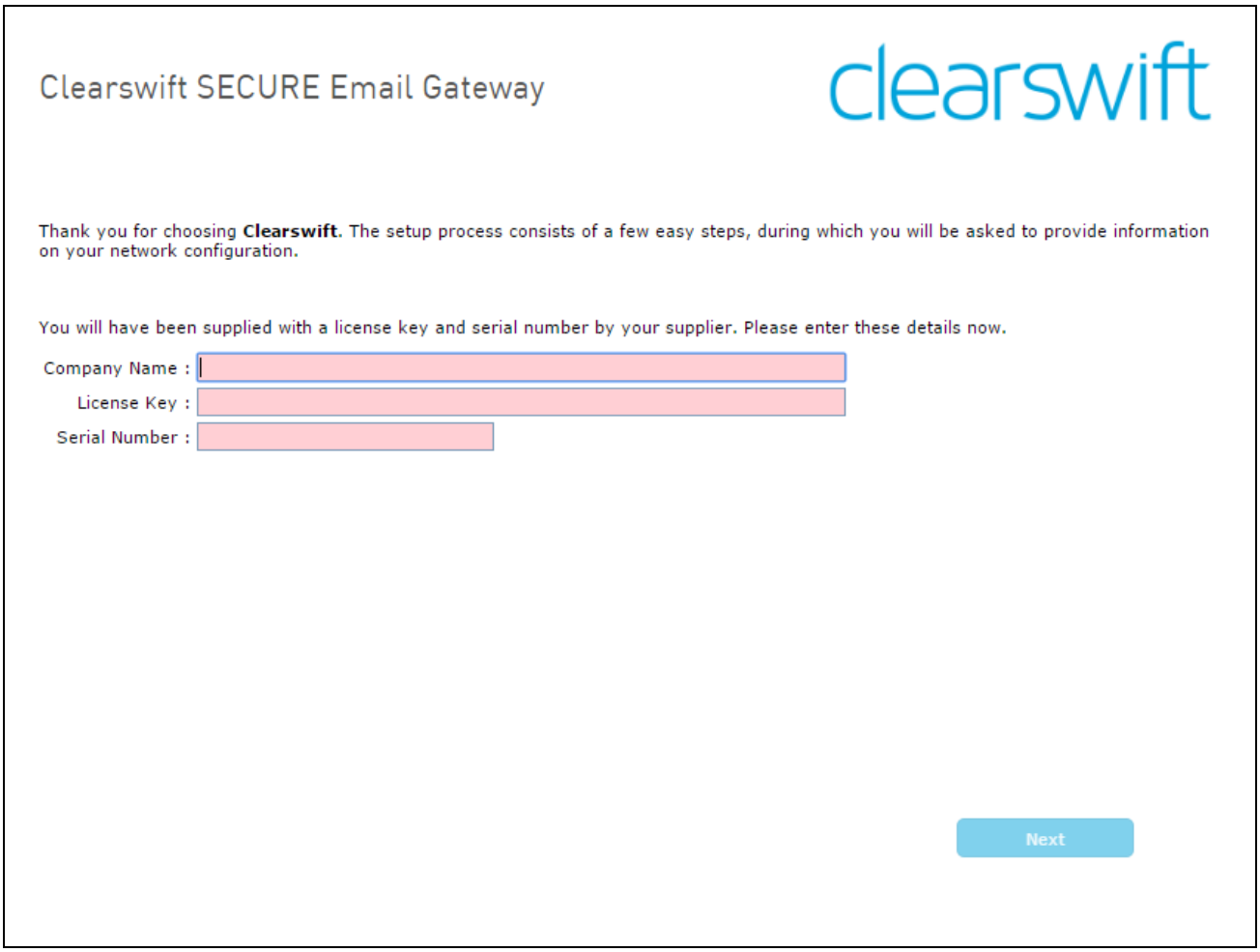
6. Apply your settings and confirm to reboot the server.
7. Following the reboot, open a browser and navigate to the Gateway IP address:

   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 Email Gateway* installation wizard is displayed.



The system might take around 5-10 minutes to apply the settings before you can use the Clearswift SECURE Email 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 Email 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.

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. Upgrading from an earlier version

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

If you are migrating from a previous version of the Clearswift SECURE Email Gateway, you ***must***:

1. Apply any pending configuration changes.
2. Back up your system and latest configurations before installing.
3. Clear the inbound queues.

If you are upgrading from the most recent version (4.9.0):

Check your email routing. On upgrade, the Gateway migrates routes with the same domain to **MTA Groups**.

If you are upgrading from version 4.6.0 or earlier:

Check your email routing.

On upgrade, the Gateway migrates your existing routes by collecting together any routes with the same domain (routing to different servers). These are added to MTA Groups and are used sequentially as failovers. This transfers your pre-existing failover configuration into the MTA Group format.

The Gateway then groups any identical routes (Server, Port, Auth, and TLS) that route to different domains. This helps you to identify routes more easily on the **MTA Groups** tab.

4.5 Applying software updates

Perform the following steps to download and apply software updates when you upgrade to Clearswift SECURE Email Gateway4.10.0.

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 Email 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.

To apply software updates:

1. Select **Configure System** > **View and Apply Software Updates** > **Apply Updates** > **OK** from the Clearswift Server Console main menu.
2. Select **Yes** to confirm that you want to apply the updates.
   All downloaded updates will now be installed. This process can take several minutes. A rolling progress log will be displayed.
3. When the *Operation Complete* message appears, select **Done** to complete the install process.

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

Gateway services will restart automatically in either case.

4.5.1 Upgrading Kaspersky

After the Gateway software has been upgraded, traffic is stopped while the anti-virus definitions are updated. Traffic will be restarted automatically afterward. However, if you do not have a reliable connection to the Internet or are working in an offline environment, the definitions cannot be updated and traffic will not be restarted.

You can choose to get the definitions yourself by other means, or to restart the traffic with out-of-date definitions.

To restart traffic manually:

1. Navigate to **System** > **Service Control**.
   The **Service Control** page is displayed.
2. Click **Restart** for the stopped **Policy Enforcement** service.

A dialog appears indicating whether the action has been successful.

You may have to wait a few moments before the requested action completes. When the status changes, the **Current Status** table indicates the new status.

4.5 Upgrading Users from version 4.8 or earlier

After you have upgraded, you need to assess the names of the roles created for your existing users as part of the transition to role-based administration. The upgrade process identifies all unique roles and gives them names, such as Role 1, Role 2, linking them up with the relevant users.

It is recommended that you give the roles more meaningful names after you have upgraded.

4.5 Upgrading TLS configuration from version 4.6 or earlier

When you upgrade, mail flow is stopped. You must modify the mandatory Outbound TLS settings in your Connection Profiles before you can enable mail flow by restarting the **SMTP Inbound Transport**, **SMTP Outbound Transport**, and **SMTP Alert Transport** services.

1. Check if you are using custom Sendmail configuration files. These are **customin.m4** and **customout.m4** files in **/etc/mail**. You are advised to contact Clearswift Support to discuss how to migrate these settings.
2. Check if you are using mandatory TLS settings. These settings will need to be modified after the upgrade. If you are using mandatory TLS settings, when you upgrade, mail flow is stopped. You must:
   - Configure mandatory Outbound TLS settings on individual Connection Profiles. Specify the Connection Profile for each routing table entry in the Email Routing page that requires a mandatory TLS connection.
   - Ensure that for Outbound TLS, SAN/CN matching values do not include whitespace characters.
   - Restart mail flow by starting the following services: SMTP Inbound Transport, SMTP Outbound Transport, and SMTP Alert Transport.

   If you did not have TLS configured prior to upgrade, disregard this step.
3. Check your email routing failover procedures. Postfix does not attempt multiple routing table entries on initial failure and must be set up so that routing is performed by DNS, using a DNS record for the domain with multiple "A" records. Ensure that your failover procedures take this into account. For more information, refer to Specifying Routing of Email.
4. If you are using address rewriting, note that the Validate Sender Domain check is now performed on the original address, not the rewritten address.

5. Change your AUTH profile user names and passwords, if you are using the same user name on different profiles. For more information, refer to SMTP Authentication.
6. Perform maintenance on the Connection Profile client host list and sender domain list. Sender domains are configured separately.
   On upgrade, anything other than an IP address is placed on both lists and requires that you remove the domains from the client host list and the hosts from the sender domain list. For more information, refer to Manage SMTP Connections.

Appendix A: Software install process (from disc)

The following steps describe how to install the Clearswift SECURE Email Gateway on top of an existing Red Hat Enterprise Linux (RHEL) 6.10 Server (including a suitably configured AWS or Azure instance) using the ISO image.

You should install RHEL 6.10 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.

To install the Clearswift SECURE Email 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 Email Gateway:

```
rpm -ivh /media/os/cs-repo/Packages/cs-email-repo-conf-
3.6.3-1.x86_64.rpm
```

4. Forcibly remove postfix, rsyslog and samba V3:

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

5. Install the required product using the following command:

```
yum install -y cs-email --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 Email Gateway user interface. See Configuring SSH Access in the Clearswift SECURE Email 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 Email Gateway on top of an existing Red Hat Enterprise Linux (RHEL) 6.10 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 6.10 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.

To install the Clearswift SECURE Email Gateway:

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 package:

```
# curl --get --remote-name
http://repo.clearswift.net/rhel6/gw/os/x86_64/Packages/cs-
email-repo-conf-3.6.3-1.x86_64.rpm
```

```
% Total    % Received % Xferd  Average Speed   Time    Time
   Time  Current

Speed

101  5084  101  5084    0     0   702k      0 --:--:-- --:-
-:-- --:--:-- 1654k
```

3. Download an install the Clearswift GPG public key:

```
rpm --import http://repo.clearswift.net/it-pub.key
```

4. Verify that the downloaded cs-email-repo-conf package is as expected before it is installed:

```
# rpm --checksig --verbose cs-email-repo-conf-3.6.3-1.x86_
64.rpm
```

```
Header V4 RSA/SHA1 Signature, key ID 5522142c: OK

Header SHA1 digest: OK
(bd504da4d39883f6f001e058c6e8cc506ea1fddc)

Header V4 RSA/SHA1 Signature, key ID 5522142c: OK
```

```
Header SHA1 digest: OK
(bd504da4d39883f6f001e058c6e8cc506ea1fddc)

V4 RSA/SHA1 Signature, key ID 5522142c: OK

MD5 digest: OK (77df2321e573ac1d8e57578cf6f91a8c)
```

The numbers shown in the example above may be different to those displayed in the terminal window.

5. 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 Email Gateway.

```
rpm -ivh cs-email-repo-conf-3.6.3-1.x86_64.rpm
```

6. Forcibly remove postfix, rsyslog and samba V3:

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

7. Install the required product using the following command:

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

8. 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 Email Gateway user interface. See Configuring SSH Access in the Clearswift SECURE Email 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 Email Gateway software ISO image to USB media.

1. Download the Clearswift SECURE Email Gateway software ISO image from the Clearswift download area.

Please ensure you are using the correct version of the ISO image: EMAIL_4100_4100.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 Email 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 Email 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 Email Gateway to complete the installation process.

Appendix D: How to re-enable TLS v1.0 and update ciphers on the 4.10.0 Gateway

The following steps describe how to re-enable TLS v1.0 and update ciphers if they have been affected by prior installation, upgrade or other activities.

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
```

Appendix E: Firewall Ports

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

Port	Protocol	Direction	Required for
20	FTP	In/Out	Backup & Restore if using an FTP server located beyond the firewall.
21	FTP	In/Out	Backup & Restore and Transaction Logging if using an FTP server located beyond the firewall.
21	FTPS (exp)	In/Out	Backup & Restore and Transaction Logging.
22	TCP	In	SSH access to the console.
22	SFTP	Out	Backup & Restore, and, server containing lexical data for import
25	TCP	In	Inbound SMTP
25	TCP	Out	Outbound SMTP. If your system uses an alternative port, open that instead.
53	UDP/TCP	In/Out	TRUSTmanager LiveFeed checks
53	UDP/TCP	Out	DNS requests, if using DNS servers beyond the firewall. Only allow outbound requests to the specified DNS servers, and responses from those servers.
80	TCP	In	HTTP access to the PMM interface (if 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,**

Port	Protocol	Direction	Required for
			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-update-8-4.clearswift.net, kav-update-8-5.clearswift.net, kav-update-8-6.clearswift.net**
80	TCP	Out	HTTP access to the ClearswiftJunk Email and Malware Detection Servers
80	TCP	Out	HTTP access to the policy rule/engine and spam update servers
80	TCP	Out	Clearswift Spam Detection stats from clearswiftstat.mailshell.net
80	TCP	Out	Access to SpamLogic Rule/Engine updates sn12.mailshell.net, db11.spamcatcher.net, verio.mailshell.net, ruledownloads.mailshell.net, tisdk.mailshell.net
80	TCP	Out	HTTP access to 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

Port	Protocol	Direction	Required for
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 Email Gateway web interface and for communications between Peer Gateways
443	TCP	Out	HTTPS access to the Clearswift Update Server for TRUSTmanager statistics.
443	TCP	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)
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)
11371	TCP	In/Out	HTTPS Key Server Queries
19200	UDP	In/Out	Broadcasting of greylisting data to Peer Gateways