clearswift
RUAG Cyber Security

Clearswift SECURE Web Gateway
Installation & Getting Started Guide

Version 4.7.2

Document Revision 1.0

Copyright

Contents

1. About this guide

This guide provides information for administrators installing the Clearswift SECURE Web 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 Web Gateway for the first time.
- Existing customers upgrading from the most up to date version 3.2 release of the Clearswift SECURE Web Gateway to a 4.7.2 release.
- Existing customers upgrading from an earlier version 4 release of the Clearswift SECURE Web Gateway to version 4.7.2.

2. Before installing

This section outlines prerequisites and considerations you need to make before installing the Clearswift SECURE Web Gateway . The Gateway runs on 64 bit Red Hat Enterprise Linux (RHEL 6.9). You can install the product on a physical server or virtual machine. See Prerequisites for more information on supported platforms.

2.1 Types of installation

You can install the Clearswift SECURE Web 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 6.9 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 6.9 platform.	Appendix A: Software Install Process
Software install process (from online Clearswift repositories)	Applies to users installing the product on an existing RHEL 6.9 platform.	Appendix B: Software Install Process

2.2 Obtaining the software

You can obtain the Clearswift SECURE Web Gateway software from:

- The Clearswift download area where you can download the Clearswift SECURE Web 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 6GB RAM and a 60GB hard drive for use in testing and demonstration environments. Clearswift recommends a minimum of 8 GB RAM and 200GB hard drive for use in a production environment based on your storage and processing requirements. See

the SECURE Web Gateway v4 Sizing Guide for further information on the hardware sizing guidelines.

Installation media

Please ensure you are using the correct version of the ISO image: WEB_472.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 Web 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 Web Gateway UI 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)

3. Installing the Clearswift SECURE Web Gateway

You can install the Clearswift SECURE Web 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 6.9 operating system and the Clearswift SECURE Web 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 Web Gateway

The following steps describe how to install the Clearswift SECURE Web 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 6.9 and the Clearswift software.

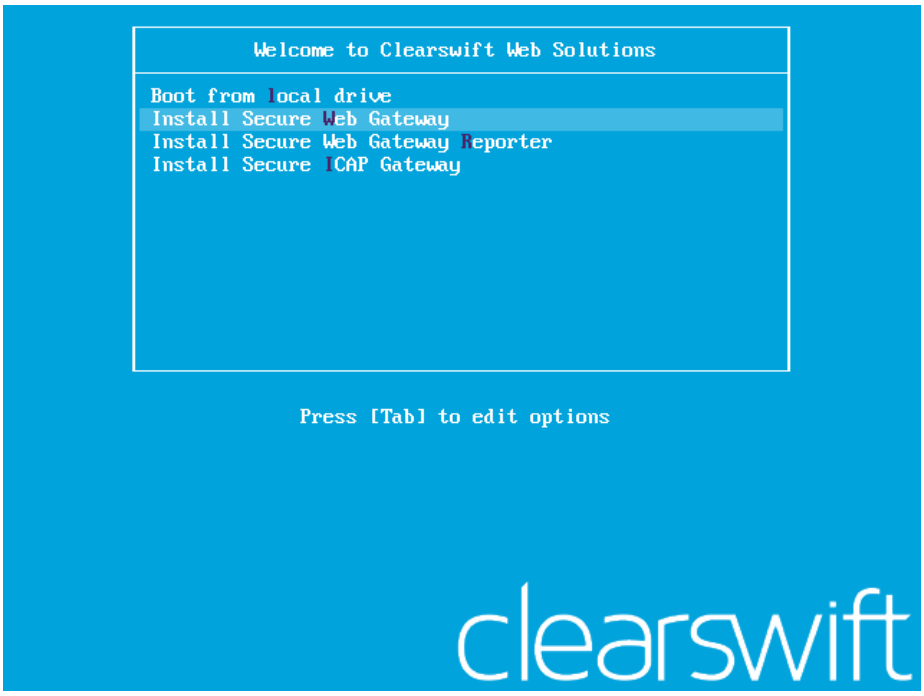
If you are performing the hardware install, go to Section 3.3 Running the Clearswift System Configuration wizard.

If you are installing onto an existing RHEL 6.9 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 Web 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 Web 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 Web 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 Web 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 Web Gateway on a hosted Microsoft Azure platform, we recommend reviewing the section on **How to change your network settings** in the Clearswift SECURE Web Gateway with Microsoft Azure Installation Guide.
>
> For optimum web-browsing performance and anti-virus scanning, the Gateway requires access to a fast DNS server.

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.

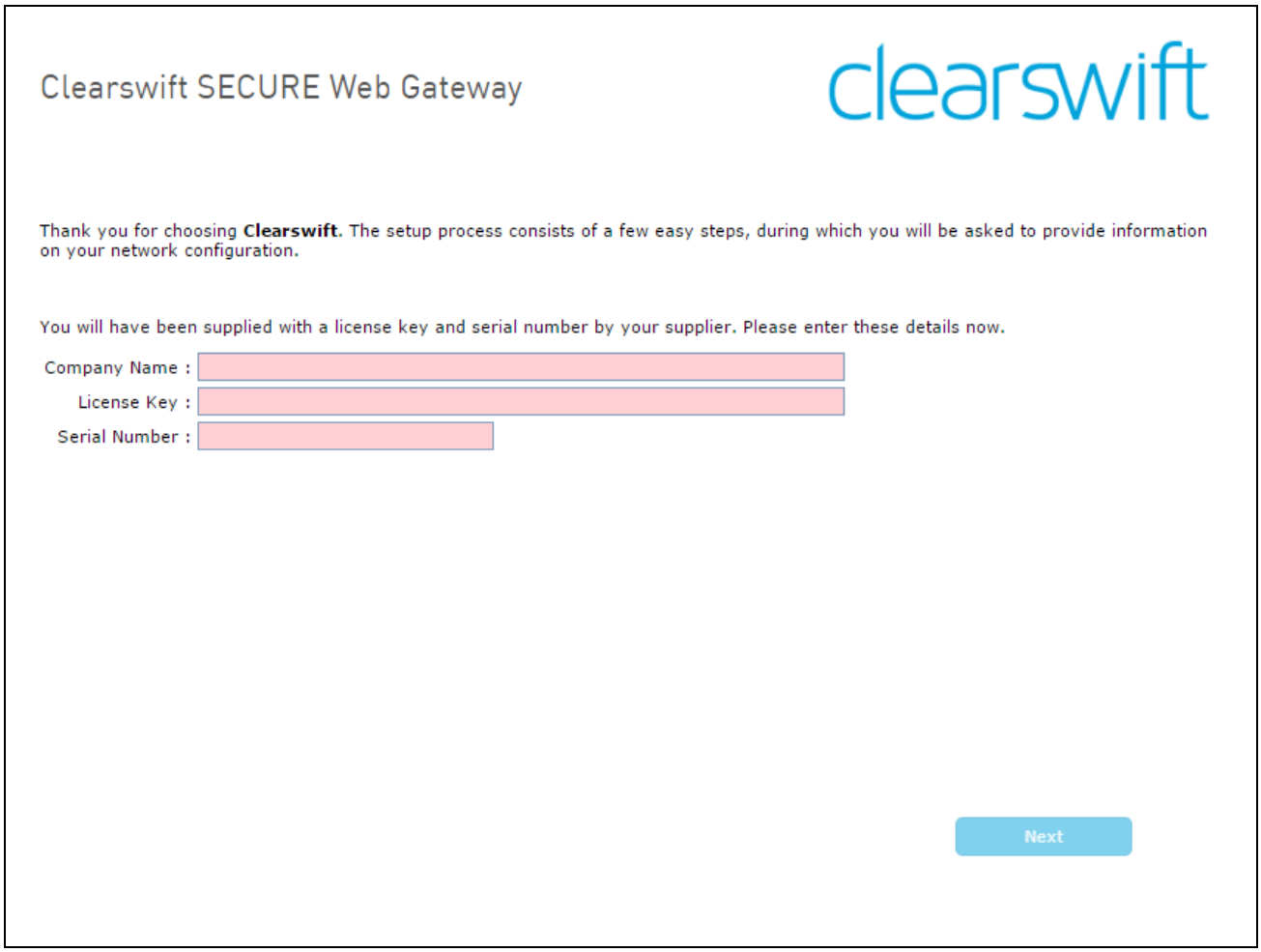
6. Apply your settings and confirm to reboot the server.
7. Following the reboot, open a browser and navigate to the Gateway IP address:

   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 Web Gateway* installation wizard is displayed.



The system might take around 5-10 minutes to apply the settings before you can use the Clearswift SECURE Web 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 Web 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 4.7.2 Gatewayand **update the ciphers** on both the v4 and v3 Gateways.

These instructions should be applied *after* installing the 4.7.2 Gateway, and after configuring the Gateway using the *Clearswift Installation Wizard*.

3.3.1 How to re-enable TLS v1.0 on the 4.7.2 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
```

3.3.2 How to update the keystore on a v3 peer Gateway

To generate a certificate and deploy it to the KeyStore for Tomcat to use:

1. Assume root role at the command line.
2. `cd /opt/msw/data/`
3. `mv keystore keystore.orig`
4. `keytool -genkey -alias tomcat -keyalg RSA -sigalg SHA1withRSA -keystore keystore -storepass changeit --dname "CN=Clearswift,OU=Clearswift,O=Clearswift,L=Reading,S=Berkshire,C=Uk" -validity 3650`

   > Update the certificate attributes (CN, OU, O, etc.) with your own details

   After entering this command, the system prompts you for the key password for Tomcat. Press RETURN if this is the same as the KeyStore password.
5. `uiservicecontrol 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. Upgrading from an earlier version 4 release to version 4.7.2

If you are installing the Clearswift SECURE Web 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 Web Gateway 4.7.2.

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 Web 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.

Appendix: Software install process (from disc)

The following steps describe how to install the Clearswift SECURE Web Gateway on top of an existing Red Hat Enterprise Linux (RHEL) 6.9 Server (including a suitably configured AWS or Azure instance) using the ISO image.

You should install RHEL 6.9 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 Web 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-web-repo-conf package. The cs-web-repo-conf package configures your system to be ready for you to install the Clearswift SECURE Web Gateway :

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

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-swg --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 Web Gateway user interface. See Configuring SSH Access in the Clearswift SECURE Web 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: Software install process (from Clearswift online repositories)

The following steps describe how to install the Clearswift SECURE Web Gateway on top of an existing Red Hat Enterprise Linux (RHEL) 6.9 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 6.9 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 Web 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-web/os/x86_
64/Packages/cs-web-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-web-repo-conf package is as expected before it is installed:

```
# rpm --checksig --verbose cs-web-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-web-repo-conf package. The cs-web-repo-conf package configures your system to be ready for you to install the Clearswift SECURE Web Gateway .

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

6. Forcibly remove postfix, rsyslog and samba V3:

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

7. Install the required product using the following command:

```
yum install -y cs-swg --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 Web Gateway user interface. See Configuring SSH Access in the Clearswift SECURE Web 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: USB installation media preparation

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

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

   Please ensure you are using the correct version of the ISO image: WEB_472.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 Web 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 Web 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 Web Gateway to complete the installation process.

Appendix D: Web Gateway Reporter install and upgrade process

The following steps describe how to install or upgrade a peer group containing a Clearswift Web Gateway Reporter from version 3.2 to version 4.7.2. The Gateway Reporter is designed to consolidate the audit information processed by your Gateways. It is typically installed as a Gateway Peer in your network, where it is dedicated to collecting and displaying the audit information from the Web Gateways in the peer group.

Terminology

SWG	Clearswift SECURE Web Gateway
WGR	Clearswift SECURE Web Gateway Reporter
v3	Version 3 of the Clearswift Gateway appliances: typically, version 3.2
v4	Version 4 of the Clearswift Gateway appliances: in this scenario, version 4.7.2

Install a Web Gateway Reporter for the first time

If you are installing a Web Gateway Reporter, use the instructions in this install guide to install or upgrade your Clearswift SECURE Web Gateways to version 4.7.2.

When all the SWGs in the peer group have been upgraded or installed, install a Web Gateway Reporter using the same process.

Run the ISO and select **Web Gateway Reporter** from the

Welcome to Clearswift Web Solutions boot screen.

Add the Web Gateway Reporter to the peer group.

Upgrade a Web Gateway Reporter

To upgrade your existing v3 Web Gateway Reporter and successfully migrate your data alongside your Web Gateways, you need to select a migration strategy based on your environment and your requirements.

We recommend you consider your strategy carefully before you begin. You cannot change your decision or revert the changes during the upgrade process.

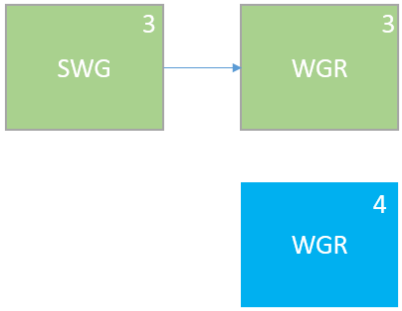
Choose a migration strategy

There are two options:

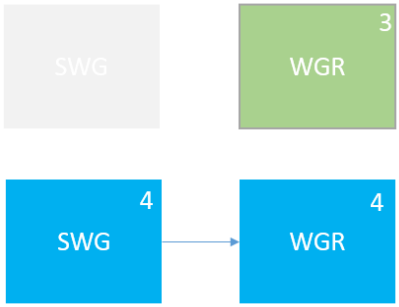
Option A: Replace and expire the v3 Web Gateway Reporter

This option avoids any slow migration steps, which might be critical if your existing Web Gateway Reporter contains a large amount of data (>30GB).

1. Add a new v4 WGR to the peer group. The existing v3 SWGs continue to send audit logs to the v3 WGR.



2. Upgrade each SWG to version 4.7.2 and add to the peer group. Each upgraded SWG sends audit information to the v4 WGR.



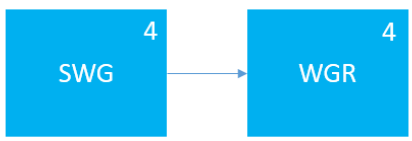
3. Leave the v3 WGR in the peer group until the data expires. Reports will include data from both versions of WGR.

Option B: Upgrade the peer group and add a v4 Web Gateway Reporter

Use this option if you have a small amount of data (<30GB) you want to migrate, or if you do not want to keep your existing v3 WGR running for a long time. Upgrading the WGR could take many hours.

1. Upgrade existing SWGs to version 4.7.2. When the upgrade is complete, each SWG consolidates audit logs locally.

2. Migrate your v3 WGR to a v4 WGR and add it to the peer group. The length of this process varies depending on the amount of information you are migrating. When the upgrade is complete, each SWG sends newly generated audit information to the new WGR. At the end of the process, the information consolidated while the WGR process took place will be kept locally in the SWGs. The newly generated information will be consolidated locally in the v4 WGR .



In either option, you can continue to run reports on your audit data during the upgrade, with the exception of data held by any peer which is in the process of migration.

How to upgrade a SECURE Web Gateway (SWG) in a peer group containing a Web Gateway Reporter

You will need to do this if you choose Option A or Option B.

1. Prevent web traffic from reaching the SWG.
2. Navigate to **System** > **Service Control**. Stop the **Web Proxy** service.
3. Wait for the audit log queue (/var/msw/proxy/audit) and the audit log export queue (/var/msw/repl/{uuid}) to clear. This should take around 15 minutes.

Use the following commands to check the queues are clear:

```
ls /var/msw/proxy/audit
```

Wait for the ***.log** files to disappear from the output.

```
ls /var/msw/msw/repl/*
```

Wait for the **web_audit_*.log** files to disappear from the output.

4. Remove the v3 SWG from the peer group.
5. Perform a system backup.
6. Use the instructions in this install guide to install a v4 SECURE Web Gateway.
7. Restore the backup to the new v4 SWG.
8. Add the v4 SWG to the peer group.

How to upgrade a Web Gateway Reporter (WGR)

You will need to do this if you choose Option B.

1. Prevent any new audit logs from reaching the v3 WGR. This can be achieved by upgrading all your v3 SWGs to version 4.7.2.
2. Wait for the audit log queues in the WGR to clear (/var/msw/proxy/audit).

Use the following commands to check the queues are clear.

There is a separate input directory for the audit logs received from each peer. Check that each directory contains no log files.

```
ls /var/msw/proxy/audit/*
```

```
/var/msw/proxy/audit/logreader.state
```

```
/var/msw/proxy/audit/peermap.properties
```

Wait for the **web_audit_*.log** files to disappear from the sub-directories.

3. Perform a system backup on the v3 WGR.
4. Restore the backup to the new v4 WGR. The length of this process varies depending on the amount of data you are restoring.
5. Add the v4 WGR to the peer group.
6. Remove the v3 WGR from the peer group.