FORTRA

Clearswift Secure Web Gateway

Version 6.1.1

Installation Guide

Copyright Terms and Conditions

202510230119

Contents

1. About this guide

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

Who is this guide for?

This guide is intended for use by:

- New and existing customers installing Secure Web Gateway version 6.1.1.
- Existing customers upgrading from version 6.x of Secure Web Gateway to version 6.1.1.

Identified issue in this release

You might encounter an error, stating “Applying updates failed”, when updating via **Cockpit** > **Software updates**. This is due to an issue with the Red Hat Cockpit component.

- To resolve the error, run `dnf upgrade` from the command line.
- For more information, see this knowledge article in the Fortra Support Portal.

2. Before installing

This chapter outlines prerequisites and considerations you need to make before installing Secure Web Gateway. Secure Web Gateway runs on 64 bit Red Hat Enterprise Linux (RHEL) 9.4. You can install the product on a virtual machine or physical server.

Types of installation

You can install Secure Web Gateway using one of the following:

Installation type	Description	Where to start
Private cloud (e.g. VMware, Hyper-V and customer hardware)	Applies to users installing the product from an ISO image that contains both RHEL 9.4 and the Gateway software.	ISO installation
Public cloud (e.g. AWS, Azure or customer supplied OS)	Applies to users installing the product on an existing RHEL 9.4 platform.	Software installation

Prerequisites

Hardware requirements

Testing and demonstration environment: Your computer or virtual machine requires a minimum of 8 GB RAM and an 120 GB hard drive.

Production environment: We recommend a minimum of 16 GB RAM and 200 GB hard drive, based on your storage and processing requirements.

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

- 1 anti-virus scanner

Product spec	CPU Cores/vCPU	RAM (GB)	Disk (GB)	Raid
Physical - Low Spec	4	16	200+	Optional
Physical - High Spec	8	32	300+	Yes
Virtual - Low Spec	4	16	200+	Optional
Virtual - High Spec	8	32	300+	Yes

Other considerations

When configuring Secure Web Gateway to scan *very* large files, system preparation and configuration can affect scanning time and outcomes.

The following should be taken into account when scan time becomes lengthy, or if scanning failures occur:

- Sizing of the Gateway should accommodate the anticipated size of files being scanned. CPU and Memory resources may need to exceed those specified in this guide, and available disk space should be, at least, double that of the largest anticipated file(s) being scanned, as the entire file needs to write to local disk and be decompressed (as applicable) before scanning can begin.
- Sizing of the Gateway should also consider the number of jobs being run in parallel and be factored into the host specification.
- **Global Size Restriction** should always be configured for the uncompressed or decompressed size of the largest anticipated file(s) being scanned.
- Scanning large files that exceed the originally configured **Global Size Restriction** will increase time to scan and may incur unexpected scanning failures, particularly when the **Detect Lexical Expression** or **Redact Text** content rules are present.
- Scanning with content rules that exceed the originally configured policy will increase time to scan and may incur unexpected scanning failures, particularly when the **Detect Lexical Expression** or **Redact Text** content rules are present.
- If a file is taking too long to scan, or is otherwise impacting the Gateway performance negatively, it is possible to discard that file by restarting the content scanning engine.
- To accommodate the large-file scanning, timeout settings for the **Content Scanning Engine Watchdog** (default for 1 GB+ is 30 minutes) might require higher values. If you consider this, please consult Clearswift prior to making changes.

Installation media

The software ISO image (`WEB-6.1.1.iso`) is available from the Fortra Support Portal. See the ISO installation chapter of this guide for more information.

3. ISO installation

If you are upgrading from version 6.x to 6.1.1, go to the Upgrade chapter of this guide.

If you are migrating from version 5.7.0 to 6.1.1, see the Migrate chapter of this guide for more information.

Before you start

Obtain the software ISO image

The software ISO image is available from the Fortra Support Portal.

- Log in to the Fortra Support Portal and select your product.
- On the **Secure Web Gateway** page, navigate to **Downloads** > **VIEW DOWNLOADS**.
- Download the Secure Web Gateway software ISO image from the Downloads page. Ensure that you are using the correct version of the ISO image (`WEB-6.1.1.iso`).

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

If you would like to copy the ISO image to USB media, see the Appendix of this guide for more information.

Additional settings for your Secure Web Gateway

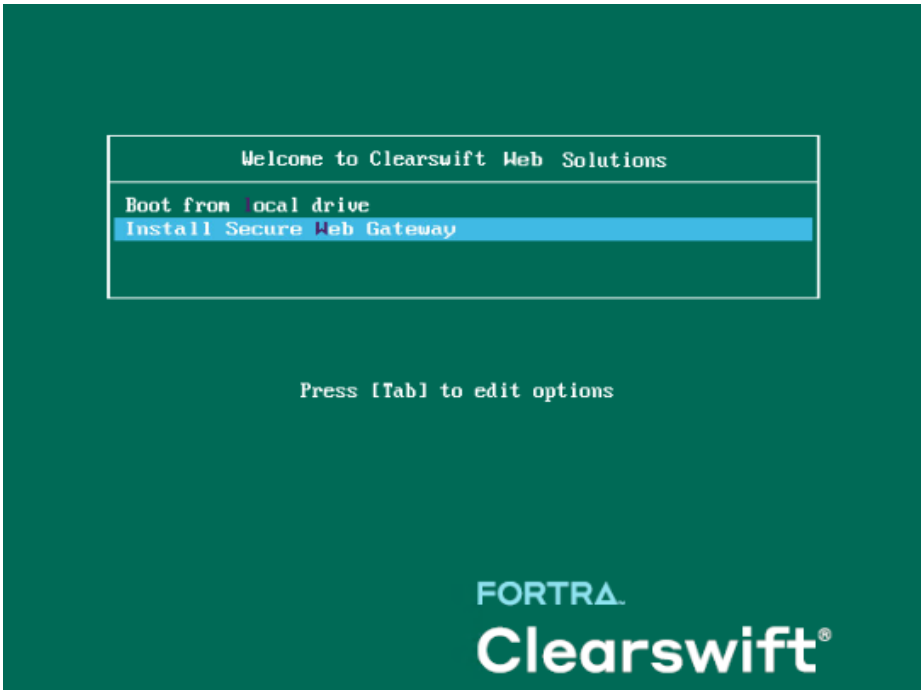
- **DISA STIG security profile**: If you wish to secure your Red Hat 9.4 server to DISA STIG compliance standards, you will need to apply this profile after installing Secure Web Gateway. See the Appendix of this guide for more information.

  STIG remediation may not be suitable for your installation. See the relevant chapter of this guide to check this.

Install RHEL 9.4 and Secure Web Gateway from the ISO image

1. Connect the ISO image or the media containing the ISO image as a bootable device.

   Power on the server. The **Welcome to Clearswift Web Solutions** menu should be displayed. If the load device can not be found, you might need to adjust your system boot sequence in the BIOS.



2. Use the arrow keys or keyboard shortcuts to select **Install Secure Web Gateway** from the menu, and then press the **Enter** key. The install process begins.
3. The **Red Hat Installation Wizard** is displayed and prompts you to select the language to be used during the installation process.
4. Configure the server. On the **INSTALLATION SUMMARY** page:
   - Settings with ⚠ icon: these must be configured.
   - Other settings: these should not be modified unless advised by Support, as Fortra provides default configuration.
5. Set a password for the root user account and create an additional administrator account.

   See the Create administrator accounts section of this guide for

more information.

Creating additional administrator account(s) can also be done post-installation via Red Had Cockpit.

6. We recommend configuring your network and hostname settings now.

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

7. Scroll to the bottom of the wizard configuration page.
8. Click **Network & Host Name**.
9. Select the Network Card to configure and click **Configure**.
10. Select the **IPv4** Settings tab. Select **Manual** entry and click **Add**.

As a standard, we recommend configuring each network card with a static network address, but you could leave this automatic. Configure as per your organization's requirements.

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

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

12. You can accept the default hostname, or enter your hostname in the **Host Name** field and click **Apply**.
13. Once satisfied that the hostname and network cards are configured correctly, click **Begin Installation**. This will configure Red Hat and install the Gateway.
14. The package installation takes approximately 30 minutes. Once complete, the Gateway automatically reboots.
15. Go to the Configure Gateway chapter of this guide and continue.

There are several actions you may need to perform at this point, including configuring the online repositories.

See the Post-install actions section (under the Configure Gateway chapter) of this guide for more information.

4. Software installation

The following steps describe how to install Secure Web Gateway on top of an existing Red Hat Enterprise Linux (RHEL) 9.4 Server (including a suitably configured AWS or Azure instance).

If you are upgrading from version 6.x to 6.1.1, go to the Upgrade chapter of this guide.

If you are migrating from version 5.7.0 to 6.1.1, see the Migrate chapter of this guide for more information.

Before you start

Prerequisites for installing Red Hat 9.4

- **Software Selection**: You should install Red Hat 9.4 as a **Minimal** installation, with a separate `/(root)` and `/var` partition.
- The `root` partition should be a minimum of 20 GB, and the `/var` partition should use a minimum of 120 GB for a test environment, and 200 GB for a production environment.
- **Network & Host Name**: Ensure that your Gateway has a hostname configured. To check this, run the following:

```
hostnamectl
```

Additional settings for your Secure Web Gateway

- **DISA STIG security profile**: If you wish to secure your Red Hat 9.4 server to DISA STIG compliance standards, you will need to apply this profile after installing Secure Web Gateway. See the Appendix of this guide for more information.

STIG remediation may not be suitable for your installation. See the relevant chapter of this guide to check this.

Install from the Secure Web Gateway ISO

We recommend disabling or removing any existing repositories in

/etc/yum.repos.d/ on Secure Web Gateway as they may cause conflicts.

To install Secure Web Gateway:

1. Open a Terminal and log in as root user.
2. Insert the media containing the ISO image, or attach the ISO image to your virtual machine as a DVD drive.
3. Mount the media to /media/os:

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

4. Import the Clearswift GPG public key:

```
rpm --import /media/os/RPM-GPG-KEY-CS-PROD
```

5. Install the cs-rhel9-media package. The cs-rhel9-media package configures your system to install the Gateway from the ISO image:

```
dnf install -y /media/os/cs-iso-repo/cs-rhel9-media*.rpm
```

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

(Secure Web Gateway)

```
dnf install -y /media/os/cs-iso-repo/cs-rhel9-swg-repo*.rpm
/media/os/cs-iso-repo/cs-rhel9-mirrors*.rpm
```

(Web Gateway Reporter)

```
dnf install -y /media/os/cs-iso-repo/cs-rhel9-wgr-repo*.rpm
/media/os/cs-iso-repo/cs-rhel9-mirrors*.rpm
```

7. Enable the media repositories:

```
dnf config-manager --set-enabled cs-media,cs-rhel-9-media*
```

8. Install the required product using the following command:

(for Secure Web Gateway)

```
dnf install -y cs-swg
```

(for Web Gateway Reporter)

```
dnf install -y cs-wgr
```

If this step fails due to additional conflicts, you might need to remove the conflicting packages first using:

```
dnf remove <package name>
```

9. Reboot Secure Web Gateway.
10. Go to the Configure Gateway chapter of this guide and continue.

There are several actions you may need to perform at this point, including configuring the online repositories.

See the Post-install actions section (under the Configure Gateway chapter) of this guide for more information.

Install from the online repositories

To install Secure Web Gateway from repositories hosted online by Fortra, you will need the Internet access to them.

We recommend disabling or removing any existing repositories in `/etc/yum.repos.d/` on Secure Web Gateway as they may cause conflicts.

1. Assume root role at the command line.

When downloading and installing files, we recommend that you check the downloaded file can be verified against the vendor public key.

2. Download the packages containing the online repository configuration files:

   (Click  to open a page from where you can copy the commands and scripts.)

 (for Secure Web Gateway)

```
curl -Of https://cs-products.fortra.com/rhel9/swg/cs-rhel9-
```

```
mirrors-1.0.1.rpm
curl -Of https://cs-products.fortra.com/rhel9/swg/cs-rhel9-swg-
repo-1.0.1.rpm
```

(for Web Gateway Reporter)

```
curl -Of https://cs-products.fortra.com/rhel9/wgr/cs-rhel9-mir-
rors-1.0.1.rpm
curl -Of https://cs-products.fortra.com/rhel9/wgr/cs-rhel9-wgr-
repo-1.0.1.rpm
```

3. Download and install the Clearswift GPG public key:

```
rpm --import https://cs-products.fortra.com/RPM-GPG-KEY-CS-PROD
```

4. Verify the downloaded packages:

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

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

```
cs-rhel9-mirrors-1.0.1.rpm:

Header V4 RSA/SHA256 Signature, key ID 9c75f096: OK
Header SHA256 digest: OK
Header SHA1 digest: OK
Payload SHA256 digest: OK
MD5 digest: OK
```

(for Secure Web Gateway)

```
cs-rhel9-swg-repo-1.0.1.rpm:

Header V4 RSA/SHA256 Signature, key ID 9c75f096: OK
Header SHA256 digest: OK
Header SHA1 digest: OK
Payload SHA256 digest: OK
MD5 digest: OK
```

(Web Gateway Reporter)

```
cs-rhel9-wgr-repo-1.0.1.rpm:

Header V4 RSA/SHA256 Signature, key ID 9c75f096: OK
Header SHA256 digest: OK
Header SHA1 digest: OK
Payload SHA256 digest: OK
```

```
MD5 digest: OK
```

5. Install the downloaded repository-file packages:

```
dnf -y install cs-*.rpm
```

6. Install the required product using the following command:

(for Secure Web Gateway)

```
dnf install -y cs-swg --enablerepo=cs-*
```

(for Web Gateway Reporter)

```
dnf install -y cs-wgr --enablerepo=cs-*
```

This command temporarily enables access to the online repositories, and installs Secure Web Gateway.

If this step fails due to additional conflicts, you might need to remove the conflicting packages first using:

```
dnf remove <package name>
```

7. Reboot Secure Web Gateway.
8. Go to the Configure Gateway chapter of this guide and continue.

There are several actions you may need to perform at this point, including configuring the online repositories.

See the Post-install actions section (under the Configure Gateway chapter) of this guide for more information.

5. Configure Secure Web Gateway

After the installation, you may need to perform some actions to set up your Secure Web Gateway, and then complete the Initial Setup Wizard.

During this process, all system administration actions should be performed using Red Hat Cockpit.

When you log in to Cockpit with the root user name for the first time after the installation, you might receive an error, stating that your user name and password are incorrect, even if you used the correct credentials. To resolve this, follow the steps in the Red Hat Documentation.

You should avoid changing network configuration at the command line as Secure Web Gateway may not be notified of these changes.

If changing network configuration at the command line is necessary, please contact Support for more information.

Post-installation actions

We recommend that you consider the following after installing Secure Web Gateway, but before configuring its Initial Setup Wizard.

Configure update repositories

(Applies to all installation types: ISO installation and software installation)

By default, the online repositories are disabled after installation. This means that any updates will need to be installed using the ISO of subsequent Secure Web Gateway releases.

Alternatively, if Secure Web Gateway has access to the Internet, it can receive updates from the online repositories. Switching from offline to the online repositories gives access to Red Hat security fixes, normally within 24 hours of their publication and subsequent testing to ensure there are no compatibility issues. We recommend this for most installations. However, you should only do this if you intend to also use the online repositories for future product upgrades.

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

To enable the online repositories:

1. Log in to Cockpit using the administrator credentials. Ensure that you have the **Administrative access** (not the **Limited access**) to the account.

   To access the Cockpit administration user interface, open a supported web browser and enter the IP address of your Secure Web Gateway, on port 9090:

   `https://<ip-address>:9090`

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

Do not install updates at this point. You can install updates after completing the Initial Setup Wizard using `dnf upgrade` from the command line.

Firewall ports

(Applies to all installation types: ISO installation and software installation)

You may need to open firewall ports on your DMZ, depending on your network configuration. See Firewall ports in the Online Help for more information.

Create administrator accounts

(Applies to all installation types: ISO installation and software installation)

Before you start using the Gateway:

- Create a new (primary) administrator account
- Create a secondary administrator account - it is good practice, in case the password for the primary administrator account is lost.
- Disable the root user account as a security precaution

To do this:

1. Log in to Cockpit using the credentials created during the Red Hat installation. Ensure that you have the **Administrative access** (not the **Limited access**) to the account.

   To access the Cockpit administration user interface, open a supported web browser and enter the IP address of your Secure Web Gateway, on port 9090:

   `https://<ip-address>:9090`

2. Navigate to **Accounts** > **Create new account**.

- Enter the name of the new administrator account and a strong password that meets the criteria defined in the password policy.

3. Click the new administrator account and enable the following role and policy:
   - Ensure that you assign appropriate **Groups** (e.g. `wheel`) to the account, so it has the administrator privileges. The administrator user can switch their privileges by selecting either the **Administrative access** or the **Limited access**.
   - In the **Options** section, click **edit**. In the **Account expiration** dialog, select **Never expire account** and click **Change**.
   - In the **Password** section, click **edit**. In the **Password expiration** dialog, select **Never expire password** and click **Change**.

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

4. Log out of Cockpit and log back in using the new administrator credentials. Ensure that you have the **Administrative access** (not the **Limited access**) to the account.
5. Navigate to **Accounts**.
   - Expand the options (**...**) for the root user, and select **Lock account** to disable it.

Password policy

(Applies to all installation types: ISO installation and software installation)

See Password policy in the Online Help for more information.

crontab configuration

(Applies to software installation only)

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

Install additional software

(Applies to software installation only)

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

If you use Cockpit to update your Gateway, only Fortra-provided updates will be applied. This ensures that only trusted repositories are used during the process, and any unintended updates from third-party repositories will be blocked.

Complete the Initial Setup Wizard

Once you have gone through the post-installation actions above and have restarted Secure Web Gateway, run the Initial Setup Wizard.

If the installation media has been disconnected following the reboot, you must reconnect it before configuring the Initial Setup Wizard. The wizard requires access to the installation media to complete the setup of your Secure Web Gateway.

If you are installing from ISO, ensure that the media is mounted at `/media/os`.

1. To access the Secure Web Gateway's web user interface, open a supported web browser and enter the IP address of your Gateway:
   `https://<ip-address>`
2. The Initial Setup Wizard is displayed.
3. Complete the wizard to configure Secure Web Gateway.
4. The system might take around 5-10 minutes to apply the settings before you can use the Gateway. We recommend visiting the Configure Gateway topic in the Online Help when the interface is accessible.

Post-wizard actions

We recommend you consider the following after you ran the Initial Setup Wizard.

SSH access

If SSH access is required, you need to re-enable it through the web user interface. See SSH Access in the Online Help for more information.

DISA STIG security profile

(Applies to all installation types: ISO installation and software installation)

If you wish to secure your Secure Web Gateway to DISA STIG compliance standards, there are additional steps. See the Appendix of this guide for more information.

6. Upgrade from Secure Web Gateway 6.x

The method used for upgrading from version 6.x depends on whether you are upgrading from the ISO or the online repositories.

If you are installing Secure Web Gateway for the first time, go to the relevant chapter (ISO install or Software install) of this guide.

Upgrade from the Secure Web Gateway ISO

Use Cockpit to install the upgrade from the version 6.1.1 ISO image.

1. You must make the version 6.1.1 ISO image available to your Secure Web Gateway.

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

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

2. Once all update have been installed, you need to reboot the Gateway.

   Use the reboot option at the end of the process, or navigate to **Overview** and select **Reboot**. Alternatively, you can navigate to **Terminal** and enter a command.

During the ISO upgrade process, you might see an error, stating "PackageKit crashed" in Cockpit, which will be resolved on its own.

Refresh the screen to check if all updates have been installed successfully. Secure Web Gateway should work without issues after the reboot.

Upgrade from the online repositories

Unless "offline mode" is a very specific requirement for your system, you should upgrade Secure Web Gateway from the online repositories.

Offline mode is designed for installations that operate in a closed environment, disconnected from the Internet. To perform an offline upgrade, you require a copy of the latest release ISO mounted to suitable media (e.g. USB). If you need additional guidance, please contact Support.

To upgrade from the online repositories:

1. Ensure that your Gateway has access to the Internet and the online repositories are enabled. See the Configure update repositories section of this guide for more information.
2. Log in to Cockpit using the administrator credentials. Ensure that you have the **Administrative access** (not the **Limited access**) to the account.

   To access the Cockpit administration user interface, open a supported web browser and enter the IP address of your Secure Web Gateway, on port 9090:

   `https://<ip-address>:9090`
3. Navigate to **Software updates** and check for updates.
4. Install all updates to upgrade the Gateway.
5. Once all update have been installed, you need to reboot the Gateway.

   Use the reboot option at the end of the process, or navigate to **Overview** and select **Reboot**. Alternatively, you can navigate to **Terminal** and enter a command.

After the upgrade, you will find that your upgrade mode has been reset to "offline". Ensure that you re-enable the online repositories.

Peer support

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

- Secure Web Gateway version 6.1.1 can peer with another Secure Web Gateway version 6.1.1.
- Peer groups with mixed versions can co-exist with older versions to share reporting and other peering features, but policy may not be applied remotely.

7. Migrate from Secure Web Gateway 5.x

In-place upgrade is not supported from version 5.x to version 6.1.1.

If you wish to restore your version 5.x configuration on version 6.1.1, you must first upgrade your Secure Web Gateway to version 5.7.0 and backup your system. Then, you can install version 6.1.1 and restore the version 5.7.0 backup to version 6.1.1.

Basic steps will be:

Upgrade: Upgrade your Gateway to version 5.7.0, if you are using the older versions

Backup: Backup all the system areas

Install: Install version 6.1.1

Restore: Restore the version 5.7.0 system backup to version 6.1.1

Pre and post-migration considerations

Beware of the following before and/or after you perform the backup and restore operations.

Real-time Categorization

Real-time Categorization was deprecated in version 5.1.0 and is no longer supported from version 6.1.1 onwards. Ensure that any Real-time Categorization rules have been removed from your policies before you migrate.

FTP command "LIST" (dir)

In version 6.1.1, `-a` option has been removed from the FTP command `LIST` (`dir`). This allows Secure Web Gateway to work with certain FTP servers to perform the backup and restore operations. If the old functionality is required, create a file `/opt/cs-gateway/custom/general.properties` and add the following to it:

```
ftpSwitches=-a
```

Backup and restore version 5.7.0 to version 6.1.1

See the Backup and restore chapter of this guide for more information.

Troubleshoot upgrading

Upgrade the Japanese Secure Web Gateway to version 5.7.0

When upgrading the Japanese Gateway to version 5.7.0, it is possible that the user interface and other components may become broken.

To resolve this:

1. Edit `control_cs_gw_stats.sh` and comment out the following in the ExecStart function:

   (Click  to open a page from where you can copy the commands and scripts.)

   ```
   if [ ! "${_INFENV_INCLUDED}" ]; then . "${CS_SCRIPTS_DIR}"/_
   infenv; fi
   ```

2. Then, execute the following:

   ```
   sudo systemctl daemon-reload
   sudo systemctl restart cs-gw-stats
   sudo systemctl restart cs-gw-admin-ui.service
   ```

   After completing these steps, you will be able to backup the system and upgrade to version 6.1.1.

8. Backup and restore Secure Web Gateway

In the Secure Web Gateway's web user interface, navigate to **System** > **Configuration** > **Backup & Restore** to access the feature.

See Backup and Restore the system in the Online Help for more information.

Backup and restore version 5.7.0 to version 6.1.1

When migrating Secure Web Gateway from version 5.x to version 6.1.1, part of the process involves backup and restore operations.

Note that:

- The **User Interface Service** logs will not be restored.
- It is recommended that NTLM or Kerberos authentication is disabled on the version 5.7.0 machine before the backup. It can be enabled after the restore process. (The restore operation will still work with these authentication enabled in the backup. However, errors will be generated and the automatic-apply configuration will fail.)
- If NTLM authentication is used, it is necessary to join the domain after the restore process.

Backup and restore version 6.1.1 to version 6.1.1

If you installed a new instance of Secure Web Gateway or upgraded it from version 6.x to 6.1.1, you may still need to backup and restore your Gateway as part of regular maintenance.

Note that:

- It is recommended that NTLM or Kerberos authentication is disabled on the version 6.1.1 machine before the backup. It can be enabled after the restore process. (The restore operation will still work with these authentication enabled in the backup. However, errors will be generated and the automatic-apply configuration will fail.)
- If NTLM authentication is used, it is necessary to join the domain after the restore process.

Appendix: Install with USB installation media

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

1. The software ISO image is available from the Fortra Support Portal.
   - Log in to the Fortra Support Portal and select your product.
   - On the **Secure Web Gateway** page, navigate to **Downloads** > **VIEW DOWNLOADS**.
   - Download the Secure Web Gateway software ISO image from the Downloads page. Ensure that you are using the correct version of the ISO image (`WEB-6.1.1.iso`).

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

2. Use Fedora Media Writer to create a bootable USB. The latest version is available from https://github.com/FedoraQt/MediaWriter/releases.
3. Plug in the USB and follow the ISO installation chapter of this guide to install the product.

   If you use USB media to install the product, it is important that you follow the remaining steps before you complete the Initial Setup Wizard. Do not run the wizard at this point.

4. Go to Cockpit and verify that the USB is still mounted at `/media/os`. If not, run the following commands.
   - To verify the USB device ID:

     ```
     realpath /dev/disk/by-label/CS_RHEL_GW
     ```

   - To mount the device (in this example, assuming it is `sda1`):

     ```
     mount /mnt/sda1 /media/os
     ```

5. You can now run the Initial Setup Wizard.
6. After completing the wizard, verify your license and check that your licensed anti-virus-software services are installed.

Appendix: DISA STIG security profile

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

Fortra provides a DISA STIG security profile that is tailored to meet the Secure Web Gateway's operational requirements. This profile needs to be applied after installing Secure Web Gateway.

Before you start

STIG remediation on different installation types

Applying the DISA STIG security profile has been successfully tested on the following.

Running the profile on other VM technology or on hardware is not recommended as this can cause the OS to become unusable and require a full reinstall.

- Hyper-V
- VMware ESXi
- Azure
- AWS instances with UEFI boot mode

> STIG remediation on AWS instances that only support Legacy BIOS boot mode, such as *t2.xlarge* will fail.

Possible impact on the performance

Applying the DISA STIG security profile could reduce the performance of traffic-processing on your Secure Web Gateway . This is due to the increase in the level of auditing performed by the Red Hat audit service.

We recommend that you carefully monitor performance before and after applying the profile, and assign additional hardware resources if required.

Apply the DISA STIG security profile

After installing Secure Web Gateway:

> You can apply the profile after completing the Initial Setup Wizard, and anti-virus scanners have been installed and configured.

1. If you have not enabled the online repositories, insert your Secure Web Gateway ISO.
2. Log in to Cockpit using the credentials for your administrator account. Ensure that you have the **Administrative access** (not the **Limited access**) to the account.

   To access the Cockpit administration user interface, open a supported web browser and enter the IP address of your Secure Web Gateway, on port 9090:

   `https://<ip-address>:9090`
3. If you are using the ISO, mount it using:

   ```
   sudo mount /dev/cdrom /media/os/
   ```
4. Navigate to **Terminal**. Assume root user privileges using the following command:

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

   ```
   /opt/clearswift/platform/stig/bin/remediate-disa-stig.sh
   ```
6. Once the script has completed, you must reboot the system in order for the DISA STIG security profile modifications to be applied.
7. After the reboot, your ISO will be dismounted. Ensure that you re-mount using:

   ```
   sudo mount /dev/cdrom /media/os/
   ```
8. Return to the Configure Gateway chapter of this guide and continue.

Evaluating Secure Web Gateway

To evaluate the DISA STIG compliance rating of your Secure Web Gateway, you can generate a report.

1. Log in to Cockpit using the credentials for your administrator account. Ensure that you have the **Administrative access** (not the **Limited access**) to the account.

   To access the Cockpit administration user interface, open a supported web browser and enter the IP address of your Secure Web Gateway, on port 9090:

   `https://<ip-address>:9090`
2. Navigate to **Terminal**. Assume root user privileges using the following command:

   ```
   sudo su
   ```

3. Execute the following script:

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

4. The report will be available from:

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

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

Contact Fortra

For more information about the Fortra's Clearswift products and cybersecurity solutions, please visit our website.

You can contact us for questions, and to receive technical bulletins, updates, program fixes and other information on your Secure Web Gateway via email or Internet.

Fortra Support Portal

Fortra Support Portal offers various helpful resources, such as product documentation and knowledge articles. You can also contact our Technical Support, using the Fortra Support Portal.

For support issues, please:

- Check this guide's table of contents and topics for information that addresses your concern.
- Check the Knowledge Base in the Fortra Support Portal for information that addresses your concern.
- Gather and organize as much information as possible about the problem, including job/error logs, screenshots or anything else to document the issue.