FORTRA

Clearswift Secure ICAP Gateway

Version 6.0.0

Installation Guide

Copyright Terms and Conditions

202503071227

Contents

1. About this guide

This guide provides information for administrators installing Clearswift Secure ICAP 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 ICAP Gateway version 6.0.0.

2. Before installing

This chapter outlines prerequisites and considerations you need to make before installing Secure ICAP Gateway. Secure ICAP 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 ICAP 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 ICAP 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

Installation media

The software ISO image (`ICAP-6.0.0.iso`) is available from the Fortra Support Portal. See the ISO installation chapter of this guide for more information.

3. ISO installation

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 ICAP Gateway** page, navigate to **Downloads** > **VIEW DOWNLOADS**.
- Download the Secure ICAP Gateway software ISO image from the Downloads page. Ensure that you are using the correct version of the ISO image (`ICAP-6.0.0.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.

Additional settings for your Secure ICAP 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 ICAP Gateway, but before configuring its Initial Setup Wizard. See the Appendix of this guide for more information.

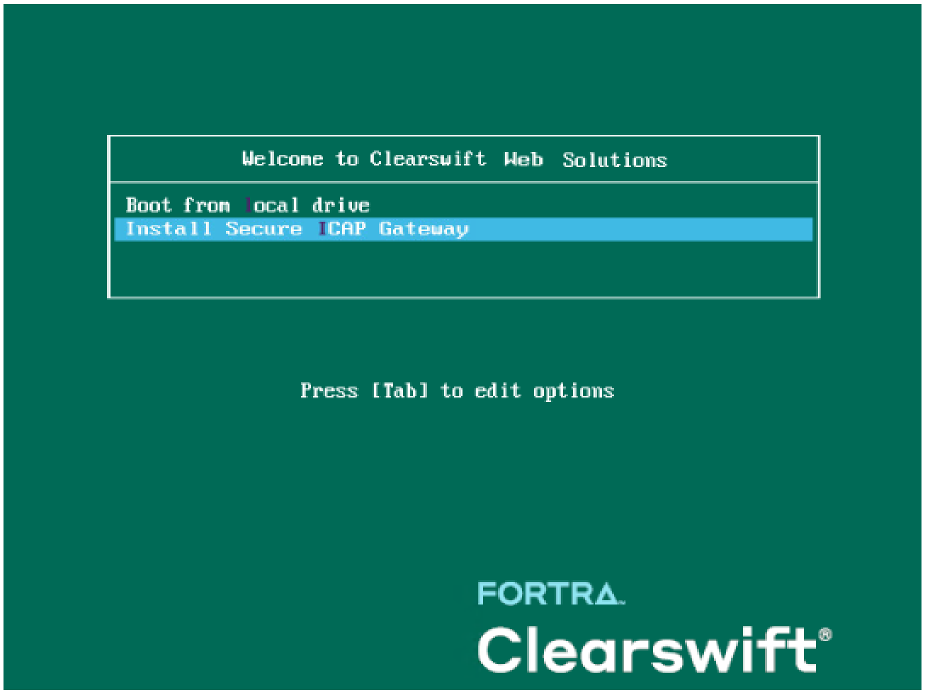
  ⓘ Applying the DISA STIG security profile has been successfully tested on Hyper-V and VMware ESXi.

  Running this profile on other VM technology (e.g. AWS) or on hardware is not recommended as this can cause the OS to become unusable and require a full reinstall. We continue to work on this area for future releases.

Install RHEL 9.4 and Secure ICAP Gateway from the ISO image

1. Connect the ISO image as a bootable device and 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.


Welcome to Clearswift Web Solutions
Boot from local drive
Install Secure ICAP Gateway
Press [Tab] to edit options
FORTRA
Clearswift

2. Use the arrow keys or keyboard shortcuts to select **Install Secure ICAP 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. The wizard starts the configuration of the server. Any of the settings may be changed, but must be provided for any option marked with a warning ⚠ icon.
5. 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 applying the **DISA STIG security profile**.
>
> 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 ICAP Gateway on top of an existing Red Hat Enterprise Linux (RHEL) 9.4 Server (including a suitably configured AWS or Azure instance).

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 ICAP 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 ICAP Gateway, but before configuring its Initial Setup Wizard. See the Appendix of this guide for more information.

> Applying the DISA STIG security profile has been successfully tested on Hyper-V and VMware ESXi.
>
> Running this profile on other VM technology (e.g. AWS) or on hardware is not recommended as this can cause the OS to become unusable and require a full reinstall. We continue to work on this area for future releases.

Install from the Secure ICAP Gateway ISO

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

To install Secure ICAP Gateway:

1. Open a Terminal and login as root user.
2. Insert the media containing the ISO image and mount it onto `/media/os`:

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

3. Import the Clearswift GPG public key:

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

4. 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
   ```

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

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

6. Enable the media repositories:

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

7. Install the required product using the following command:

   ```
   dnf install -y cs-sig
   ```

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

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

8. Reboot Secure ICAP Gateway.
9. Go to the Configure Gateway chapter of this guide and continue.

   There are several actions you may need to perform at this point, including applying the **DISA STIG security profile**.

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

Install from the Clearswift online repositories

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

We recommend disabling or removing any existing repositories in `/etc/yum.repos.d/` on Secure ICAP 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.)

```
curl -Of https://cs-products.fortra.com/rhel9/sig/cs-rhel9-mirrors-1.0.0.rpm

curl -Of https://cs-products.fortra.com/rhel9/sig/cs-rhel9-sig-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-1.0.0.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
```

```
cs-rhel9-sig-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:

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

   This command temporarily enables access to the online repositories, and installs Secure ICAP 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 ICAP 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 applying the **DISA STIG security profile**.

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

5. Configure Secure ICAP Gateway

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

Over 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 ICAP Gateway may not be notified of these changes.
>
> If changing network configuration at the command line is necessary, please contact Fortra's Clearswift support for more information.

Post-installation actions

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

DISA STIG security profile

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

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

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.

Password policy

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

See Clearswift password policy 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 ICAP 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.

Configure update repositories

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

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

Alternatively, if Secure ICAP 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. Enter the Cockpit URL into a supported web browser to load the Cockpit administration user interface, then login using the administrator credentials. Ensure that you have the **Administrative access** (not the **Limited access**) to the account.
2. Navigate to **Clearswift**. From **Product Actions** > **Enable online repositories**, click **Enable**.

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.

> ⓘ You will only be able to apply Clearswift-provided upgrades via Cockpit. This ensures that only trusted Clearswift repositories are used during the upgrade process, and any unintended updates from third-party repositories will be blocked during the process.

Complete the Initial Setup Wizard

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

> ❗ If the Clearswift 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 ICAP Gateway.
>
> If you are installing from ISO, ensure that the media is mounted at `/media/os`.

1. To access the Secure ICAP 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 ICAP 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.

6. Migrate from Secure ICAP Gateway 5.x

In-place upgrade is not supported from version 5.x to version 6.0.0.

If you wish to restore your version 5.x configuration on version 6.0.0, you must first upgrade your Secure ICAP Gateway to version 5.7.0 and backup your system. Then, you can install version 6.0.0 and restore the version 5.7.0 backup to version 6.0.0.

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 6.0.0

Restore: Restore the version 5.7.0 system backup to version 6.0.0

To perform these operations, use the **Backup & Restore** feature.

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

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

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 6.0.0 onwards. Ensure that any Real-time Categorization rules have been removed from your policies before you migrate.

FTP command "LIST" (dir)

In version 6.0.0, `-a` option has been removed from the FTP command `LIST` (`dir`). This allows Secure ICAP 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 & Restore version 5.7.0 to version 6.0.0

Note that:

- The **User Interface Service** logs will not be restored.

Troubleshoot upgrading

Upgrade the Japanese Secure ICAP 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.

Workaround

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 6.0.0.

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 ICAP Gateway's operational requirements. You can apply this profile after installing Secure ICAP Gateway, but before configuring its Initial Setup Wizard.

> ❗ Applying the DISA STIG security profile has been successfully tested on Hyper-V and VMware ESXi.
>
> Running this profile on other VM technology (e.g. AWS) or on hardware is not recommended as this can cause the OS to become unusable and require a full reinstall. We continue to work on this area for future releases.

> ⓘ Before applying this security profile, please be aware that the performance of traffic-processing on your Secure ICAP Gateway could be reduced.
>
> 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 ICAP Gateway, but before configuring its Initial Setup Wizard:

1. If you have not enabled the online repositories, insert your Secure ICAP 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 ICAP 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 ICAP Gateway

To evaluate the DISA STIG compliance rating of your Secure ICAP 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 ICAP 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 Fortra's Clearswift 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 ICAP 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.