clearswift
by HelpSystems

Installation & Getting Started Guide
Clearswift ARgon for Email
Version 5.4.3

Copyright Terms and Conditions

Contents

1. About this guide

This guide provides information for administrators installing Clearswift ARgon for Email 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 Clearswift ARgon for Email for the first time.
- Existing customers upgrading from an earlier version of Clearswift ARgon for Email to version 5.4.3.

1.2 What is Clearswift ARgon for Email?

Clearswift ARgon for Email provides an Adaptive Data Loss Prevention (A-DLP) solution that is designed to sit alongside existing email security infrastructure. Clearswift ARgon for Email complements existing email security and Data Loss Prevention (DLP) solutions by adding Adaptive Redaction features including data redaction, document sanitization and structural sanitization.
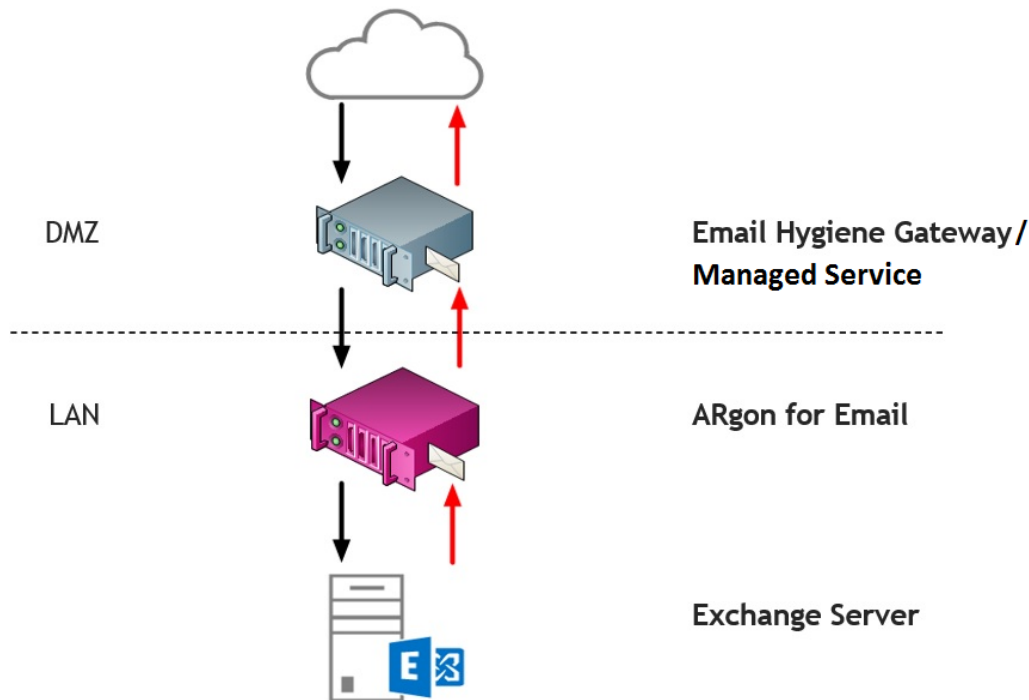
2. Before installing

This section outlines prerequisites and considerations you need to make before installing Clearswift ARgon for Email. ARgon for Email runs on 64 bit Red Hat Enterprise Linux (RHEL 7.8). You can install the product on a physical server or virtual machine. See Prerequisites for more information on supported platforms.

2.1 Types of installation

You can install Clearswift ARgon for Email using one of the following processes:

Installation process	Description	Where to start
Private Cloud (e.g. VMware, Hyper-V and customer source hardware)	Applies to users installing the product from an ISO image that contains both RHEL 7.8 or above and the Clearswift software.	Installing from the ISO image
Public Cloud (AWS, Azure or customer supplied OS)	Applies to users installing the product on an existing RHEL 7.8 or 7.9 platform.	Appendix A: Software Install Process
Customer Supplied Hardware	Applies to users deploying the product using their own hardware.	Configuring the Gateway

2.2 Prerequisites

Before installing, you should check that you have the following:

2.2.1 Hardware requirements

Your computer or virtual machine requires a minimum of 8 GB RAM and an 80 GB hard drive for use in testing and demonstration environments.

Clearswift recommends a minimum of 200 GB hard drive for use in a production environment based on your storage and processing requirements.

For a production environment, Clearswift recommends the following based on your storage and processing requirements where your ARgon for Email is configured so that your policy has:

- Optical Character Recognition (OCR) disabled

Type Email	Estimated Throughput	CPU Cores/vCPU	RAM (GB)	Disk (GB)	Raid
Physical - Low Spec	Under 20,000 msgs/hour	2	16	200+	Optional
Physical - High Spec	75,000 msgs/hour	4	16	300+	Yes
Virtual - Low	Under 20,000	2	10	200+	Optional

Type Email	Estimated Throughput	CPU Cores/vCPU	RAM (GB)	Disk (GB)	Raid
Spec	msgs/hour				
Virtual - High Spec	75,000 msgs/hour	4	16	300+	Yes

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

2.2.2 Installation media

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

- ARGON-5.4.3.iso

> After downloading the ISO image, it is recommended that an MD5/SHA hash is generated and compared to the published hashes from the download area.

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

- Copying the ISO image to USB media. See Appendix C of this guide for instructions.
- Attaching the ISO image as a virtual DVD drive. This applies to virtual machines only.

2.2.3 Browser support

Clearswift ARgon for Email supports connections using TLS 1.2 ciphers and has been tested with the following browsers:

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

3. Installing Clearswift ARgon for Email

You can install the Clearswift ARgon for Email software from the ISO image that you downloaded from the Clearswift download area.

3.1 Installing Red Hat 7.8 and ARgon for Email from the ISO image

1. Connect the ISO image or USB device as a bootable device and power on the server.

   The **Welcome to Clearswift Email 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 ARgon for Email** from the menu. Press the **Enter** key to select the installation.

   The install process begins and starts the **Red Hat Installation Wizard**.

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 then begins 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. We recommend that you configure your network and host name 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.

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

> ⚠ We strongly recommend configuring each network card with a static network address.

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

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

11. Enter your host name in the **Host name** field and click **Apply**.

3.2 Starting the installation

1. Once satisfied that the host name and network cards are configured correctly, click **Begin Installation**.
2. During the installation process, you are prompted to set the root user password and create an additional administrator account.
    - We strongly recommend entering a strong password for root and any other users that are created.
3. You must create at least one additional user who is an administrator.
    - This can also be done post-installation via Red Hat Cockpit.
    - It is good practice to create a backup administrator user in case the primary administrator password is lost.

> Ensure that you keep a record of the password expiry for any created users 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. The package installation takes approximately 15-20 minutes to complete.
   - Once complete, the Red Hat Installation Wizard automatically reboots.

3.3 Configuring ARgon for Email

On restart, you will need to complete the Clearswift ARgon for Email Installation Wizard.

1. Open a supported web browser and navigate to the ARgon for Email IP address:

   https://<ip-address>/Appliance

2. ARgon for Email Installation Wizard is displayed.

> If the Clearswift installation media has been disconnected following the reboot, you must ensure that it is reconnected before configuring the Installation Wizard. The wizard requires access to the installation media to complete the setup of your ARgon for Email.

3. Complete the wizard and click **Apply**.

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

3.4 Creating administrator accounts

Before you start using your ARgon for Email, we strongly recommend the following actions:

   - Create a new administrator account to administer ARgon for Email
   - Disable the root user account as a security precaution

This can be achieved using Red Hat Cockpit.

1. Enter the following URL into a supported web browser to load the Cockpit administration user interface:

https://<ip-address>:9090

2. Log in to Cockpit using the credentials created during the Red Hat installation, ensuring the **Reuse my password for privileged tasks** option is selected.

> (i) On first login you will be asked to change the user password. Once this has been done you should log out and then log back in, otherwise you will not have full administrator privileges.

3. Navigate to **Accounts** > **Create New Account**.
   - Enter the name of the new administrator account and a strong password that meets the criteria defined in Appendix E: Password Policy.

4. Click the new administrator account and enable the following role and policy:
   - Enable the **Server Administrator** role.
   - Select **Never lock account**. In the **Account Expiration** dialog, select **Never lock account** and click **Change**.
   - Select **Never expire password** or the **date** on which the password will expire. In the **Password Expiration** dialog, select **Never expire password** and click **Change**.

5. Log out of Cockpit and log back in using the new administrator credentials, ensuring you have selected the **Reuse my password for privileged tasks** option.

6. Navigate to **Accounts** and click the **root** user.
   - Select the **Lock Account** option to disable the root user.

> 💡 It is good practice to create a secondary administrator account, just in case the password of the primary administrator account is lost. This can be achieved by repeating steps 4 and 5.

3.5 Configuring update repositories

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 ARgon for Email releases.

Alternatively, if ARgon for Email has access to the Internet, it can receive updates from the Clearswift online repositories.

- Switching from offline to 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 online repositories for future Clearswift product upgrades.

> ⚠ Be aware that enabling online repositories is an irreversible action.

Online repositories can be enabled by following the steps below:

1. Enter the Cockpit URL into a supported web browser to load the Cockpit administration user interface. Then login using the administrator credentials, ensuring you have selected the **Reuse my password for privileged tasks** option.

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

4. Upgrading from ARgon for Email 5.x

> (i) If you are installing Clearswift ARgon for Email for the first time, you can ignore this section.

The method used for upgrading from version 5.x depends on whether you are upgrading from the ISO or Online Repositories.

4.1 Upgrading from ISO

Use Cockpit to install the upgrade from the version 5.4.3 ISO image.

You must make the version 5.4.3 ISO image available to your ARgon for Email, noting that there is an ISO image per product.

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
yum clean all
```

4.2 Upgrading from online repositories

Follow the procedure detailed in the Future updates section.

> (!) After the upgrade, you will find that your upgrade mode has been reset to "offline".
>
> In Cockpit, navigate to **Clearswift**. From **Product Actions** > **Enable online repositories**, click **Enable**.

4.3 Peer support

When upgrading your ARgon for Email, the following peer support rules are applicable:

- ARgon for Email version 5.4.3 (or earlier) can peer with another ARgon for Email version 5.4.3.

- Peer groups with mixed versions can co-exist with older versions to share message tracking, reporting and other peering features, but policy may not be applied remotely.

4.4 Post-upgrade actions (after upgrading from version 5.x)

Following an upgrade of ARgon for Email, see Post-upgrade actions for important considerations and requirements .

5. Upgrading from ARgon for Email 4.x

> ⚠ **Installing ARgon for Email for the first time**:
> If you are installing ARgon for Email for the first time, you can ignore this section.

> ⚠ **Upgrading from ARgon for Email version 4.x**:
> 1. Firstly, upgrade your version 4.x ARgon Server to version 5.2.0, following instructions in this section.
> 2. Secondly, upgrade your version 5.2.0 ARgon Server to version 5.4.3, following instructions in the Upgrading from ARgon for Email 5.x section.

5.1 Preparing to upgrade

Before you attempt any kind of upgrade, you are advised to do the following:

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

5.2 Unsupported environments

The in-place upgrade of Red Hat 6 to 7 is not supported on the following platforms:

- Amazon Web Service (AWS) instances or Machine Images
- Microsoft Azure
- Microsoft Hyper-V
- Systems using a UEFI boot loader
- Systems using Integrated Dell Remote Access Controller (iDRAC)

If you are hosting your ARgon for Email software on one of these, refer to Appendix B: Resolving Upgrade Failures for further information.

5.3 Checking prerequisites

> ⚠ 4.11.2 is minimum version required to upgrade to version 5.2.0.
> You will also need to download a copy of the version 5.2.0 ISO to

> ⚠ complete an upgrade from version 4.11.2. See [Prerequisites](#) for more information.

To upgrade your ARgon for Email to version 5.x, you need to do the following:

1. Using the Clearswift Server Console, upgrade your ARgon for Email 4.x server to version 4.11.2 using the standard upgrade previously used to upgrade ARgon for Email 4.x servers.

   - This update will install the tools required to check if the server meets the necessary pre-requisites to run Red Hat 7.8 or above, to allow you to optionally perform the upgrade of Red Hat 7.8 and ARgon for Email software if met.

   - Follow the upgrade instructions in the version 4.11.2 [Installation and Getting Started Guide](#) so that your ARgon for Email is correctly configured before attempting to upgrade to version 5.2.0.

   On completion of the 4.11.2 upgrade, you will be ready to upgrade to Red Hat 7.8 and ARgon for Email 5.2.0.

2. From the Clearswift Server Console, open a Terminal Session and enter the following to assume root user privileges:

   ```
   sudo su
   ```

3. Check your ARgon for Email v5.2.0 Installation media is accessible:

   ```
   ls /media/os/cs-iso-repo
   ```

   If your installation media is not available, enter the following command and then repeat the command above:

   ```
   service autofs restart
   ```

4. Start the upgrade verification process by entering the following command:

   ```
   cs-gateway-v5-upgrade.sh
   ```

5. The upgrade process will be performed in three phases:

   - **Analyze Gateway** will check the server meets the necessary pre-requisites to upgrade Red Hat 6 to Red Hat 7.8

   Assuming the pre-requisites are met, the following phases will be run to upgrade the software:

- **Upgrade Red Hat** will perform the migration of Red Hat 6 to Red Hat 7.8
- **Upgrade Gateway** will upgrade ARgon for Email 4.x software to 5.x

```
Welcome to the Clearswift Gateway v5.0 Upgrade

During this upgrade, both the Red Hat Operating System and existing Gateway software will
be upgraded. This will be performed in the following phases:

Phase                                          Status
--------------------------------------------------------------------------------
1. Analyze Gateway                             Not Started
2. Upgrade Red Hat                             Not Started
3. Upgrade Gateway                             Not Started

Throughout this upgrade, your Clearswift SECURE Gateway V5 ISO must be available.

The full upgrade process could take several hours to complete.

Are you ready to continue (y/n)? _
```

6. Enter **y**(es) to start the upgrade process. You will be prompted to select if you want to:
   - Check if the ARgon Server can be upgraded but upgrade later
     - This is useful if you want to understand what steps you will need to plan for before you are ready to upgrade
   - Check if the ARgon Server can be upgraded and upgrade now

```
Before the Gateway can be upgraded an analysis will be run; this can take several hours.

You can choose to upgrade the Gateway without further intervention, or to just perform
the analysis and do the upgrade later.

Please choose:

    0 - exit now
    1 - only run the analysis
    2 - run the analysis and upgrade the Gateway if possible

Please enter 0 to exit, 1 to analyse or 2 to upgrade:  _
```

7. Presuming you have entered option 1 or 2 at the prompt, the Red Hat analysis process begins.

> ⊙ This process can take several hours to complete. Do not restart your ARgon for Email while it is under analysis.

At the end of the process, you will be notified if the server can or cannot be upgraded to Red Hat 7.8.

> (!) In the event of your ARgon for Email not meeting the necessary pre-requisities to be upgrade, refer to Appendix B: Resolving Upgrade Failures.

5.4 Upgrading ARgon for Email

Follow the steps below to continue upgrading Red Hat 6 to 7.8.

1. If you selected to analyze only, but have decided to continue with the upgrade, you can restart the upgrade by entering the following command line:

```
cs-gateway-v5-upgrade.sh
```

2. The upgrade process will prompt you to reset the root user password.

> (!) You must reset the root password unless you know the existing password and have verified you can login to this server using it.
>
> This is temporarily required to allow you to log in to Red Hat Cockpit and create new administrator account(s) that you will then use to administer ARgon for Email from a Terminal session.

Once you have created these new accounts, you are strongly recommended to disable the root user account as a security precaution.

> (!) The cs-admin user that you would have used to administer ARgon for Email from a version 4.x Terminal Session is no longer available in ARgon for Email version 5.0.0 onwards.

3. The upgrade of Red Hat 6 to 7.8 will now begin. The server will reboot midway through and then complete the upgrade during the server restart.

> (i) Make sure your installation media is connected.

4. The upgrade process should take between 15-30 minutes. During this time, your ARgon Server will automatically reboot several times. You can access the

ARgon for Email Web UI once the upgrade is complete.

5.5 Post-upgrade actions (after upgrading from version 4.x)

The Red Hat and ARgon for Email upgrade process should now have completed.

You can verify this by logging into the terminal session using your root user credentials and entering the following command:

```
cs-gateway-v5-upgrade.sh
```

After the final reboot there will be a delay of approximately 10 minutes whilst the ARgon Server initializes.

5.5.1 Run a system connectivity test

Following an system upgrade, we recommend that you run the **Connectivity Test**. The test checks that the upgraded system is still capable of accessing all external resources such as AV update mirrors, DNS and similar.

> (i) To access the test, navigate to the **System** menu and select one of the sub menus, such as **Ethernet Settings** and **SSH Access**. Then, click the **Connectivity Test** in the task panel.

5.5.2 Create new administrator account(s)

Before you start using your ARgon for Email, we strongly recommend the following actions:

- Disable the root user account as a security precaution
- Create a new administrator account to administer ARgon for Email

See Creating administrator accounts for further information.

> (!) The cs-admin user account previously used in Gateway 4.x is not supported. You must use a new administrator account instead.

5.5.3 Applying the DISA STIG security profile

The DISA STIG security profile is not applied during an upgrade. To apply this profile following an upgrade see Appendix F for further instructions.

5.5.4 Future updates

You will be notified of future updates in the ARgon Administration UI and via Red Hat Cockpit.

1. Enter the following URL into a supported web browser to load the Cockpit administration user interface:

   https://<ip-address>:9090

2. Navigate to **Software Updates** and click **Check for Updates**.

See Configuring update repositories for instructions on how to enable Online Update Repositories if you would like to retrieve updates from those repositories.

> ⓘ
> Online Repositories or Offline mode?
>
> Offline mode is designed for installations that operate in a closed environment, disconnected from the Internet. Unless this is a very specific requirement for your system, you should upgrade ARgon for Email from the Clearswift online repositories.
>
> To perform an offline upgrade, you require a copy of the latest release ISO mounted to suitable media (for example, USB). Please contact Clearswift Technical Support if you need additional guidance on how to complete this step.

Appendix A: Software install process

The following steps describe how to install Clearswift ARgon for Email on top of an existing Red Hat Enterprise Linux (RHEL) 7.8 Server (including a suitably configured AWS or Azure instance).

> (i) You should install Red Hat 7.8 as a **Minimal** server installation, with a separate /(root) and /var partition. The root partition should be 20 GB (minimum) and /var should use a minimum of 80 GB for test environments and 200 GB for production environments.

> (i) If you want to secure your Red Hat 7.8 Server to DISA STIG Compliance standards, you will need to apply this profile before you continue with the ARgon for Email installation. See Appendix F for details.

Installing from the ARgon for Email ISO

To install Clearswift ARgon for Email:

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-Clearswift
```

4. Install the cs-media package. The cs-media package configures your system to be ready for you to install ARgon for Email from the ISO image:

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

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

```
yum install -y cs-rhel7-argon-email-repo cs-rhel7-mirrors
```

6. Install the required product using the following command:

```
yum install -y cs-argon-email
```

> **(i)** If the step 6 fails due to additional conflicts, you might need to remove the conflicting packages first using:
> ```
> yum remove <package name>
> ```

7. Reboot the ARgon Server and then continue from [Configuring ARgon for Email](#).

Installing from Clearswift Online Repositories

To install Clearswift ARgon for Email from repositories hosted online by Clearswift, you will need Internet access to those repositories.

1. Assume root role at the command line.

> **(i)** 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 ⬚ below to open a page from where the commands can be individually copied and pasted into your terminal:

```
curl -Of https://products.clearswift.net/rhel7/argon/cs-rhel7-mirrors-22.02.04.rpm

curl -Of https://products.clearswift.net/rhel7/argon/cs-rhel7-argon-email-repo-22.01.03.rpm
```

3. Download and install the Clearswift GPG public key:

```
rpm --import https://products.clearswift.net/RPM-GPG-KEY-Clearswift
```

4. Verify the downloaded packages:

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

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

```
cs-rhel7-argon-email-repo-22.01.03.rpm:

Header V3 RSA/SHA256 Signature, key ID 9c75f096: OK
Header SHA1 digest: OK (76fe56cb994f83cd734c6a82b13dda6ad14c59a2)
V3 RSA/SHA256 Signature, key ID 9c75f096: OK
MD5 digest: OK (7ea6a55b4b51f52401a4a513727199ea)
```

```
cs-rhel7-mirrors-22.02.04.rpm:

Header V3 RSA/SHA256 Signature, key ID 9c75f096: OK
Header SHA1 digest: OK (172adf48c2225a2b7f433584ce6705655ad47137)
V3 RSA/SHA256 Signature, key ID 9c75f096: OK
MD5 digest: OK (55a611db509e4cf522bf98f93ec3d7b3)
```

5. Manually install the downloaded repository file packages:

```
yum -y localinstall cs-*.rpm
```

6. Install the required product using the following command:

```
yum install -y cs-argon-email --enablerepo=cs-*,ext-cs-*
```

This command temporarily enables access to the Clearswift online repositories and installs ARgon for Email.

> (i) If the step 6 fails due to additional conflicts, you might need to remove the conflicting packages first using:
> ```
> yum remove <package name>
> ```

7. Enable the online repositories. See Configuring Update Repositories for more information.
8. Reboot the ARgon Server and then continue from Configuring ARgon for Email.

Post installation considerations

1. All system administration actions should be performed using Red Hat Cockpit. Enter the following URL into a supported web browser to load the Cockpit administration user interface:

    https://<ip-address>:9090

    > (!) You should avoid changing network configuration at the

> (!) command line as ARgon for Email is not notified of these changes. If changing network configuration at the command line is necessary, please contact Clearswift Support for more information.

2. If you want to secure your ARgon for Email using the DISA STIG security profile, see [Appendix F](#) for further instructions.

3. The Firewall configuration will be controlled via the ARgon administration user interface. If SSH access is required you need to re-enable it through the ARgon for Email user interface. See [SSH Access](#) in Clearswift ARgon for Email online help for more information.

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

Installing additional software

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.

> (i) 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.

Appendix B: Resolving upgrade failures

If you are unable to perform an in-place upgrade of your ARgon for Email using the instructions in Upgrading from version 4.x, the following sections provide you with some options on how to upgrade or migrate your existing policy.

ARgon for Email does not meet Red Hat 7.8 pre-requisites

If the upgrade failed because your ARgon for Email did not meet the Red Hat pre-requisites for upgrading to Red Hat 7.8, you should review the analysis report below:

- /var/log/cs-gateway/upgrades/redhat-pre-upgrade-report.txt or .html

This report will tell you the exact reasons for the failure, and in some cases provide helpful tips on how to resolve the problems.

Restoring version 4.11.1 (or later) backup to ARgon for Email 5.x

If you are unable to resolve the issues preventing you from performing an in-place upgrade, you can instead install a new ARgon for Email 5.x server and then restore a backup from ARgon for Email 4.11.1 or later.

> ⊘ Restoring a version 4.11.1 backup (or later) does not automatically restore the peer group roles so they must be restored manually.

> ⊘ It is not possible to restore a version 4.11.1 system backup on ARgon for Email later than version 5.2.0.

> 💡 See Backup and Restore the system in the Clearswift ARgon for Email online help for more information.

Appendix C: USB installation media preparation

The following steps describe how to copy the Clearswift ARgon for Email software ISO image to USB media.

1. Download the Clearswift ARgon for Email software ISO image from the Clearswift download area.

> (i) After downloading the ISO image it is recommended that a MD5/SHA hash is generated and compared with the published hashes from the download area

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. Ensure that you use the portable version.

> (i) Although you can use USB tools other than Rufus, the following USB tools will not work with the Clearswift ARgon for Email software ISO image:
> - YUMI
> - Universal USB Installer
> - Fedora liveusb-creator

The below steps assume that you are using Rufus 3.11 Portable.

3. Run **rufus-3.11p.exe**.

4. Insert your USB media and select it from the **Device** drop-down menu.

5. Under **Boot Selection**, click the **SELECT** button to choose the Clearswift ARgon for Email ISO you want to burn. Once Rufus scans the ISO, it fills in other options automatically.

> (!) When you burn the ISO, the volume label *must* be called CS_ RHEL_GW.

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 Clearswift ARgon for Email](#) to complete the installation process.

Appendix D: 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	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 using PMM)
80	TCP	Out	HTTP access to ARgon for Email 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**
161	UDP	Out	SNMP inbound: the port used by an SNMP browser when scanning ARgon for Email

Port	Protocol	Direction	Required for
162	UDP	Out	SNMP alerts
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 Key Server Queries
443	TCP	In/Out	HTTPS access to Clearswift ARgon for Email web interface and for communications between Peer Servers
443	TCP	Out	HTTPS access to the Clearswift Update Server for license management and handling Managed Lexical Expression Lists.
443	TCP	Out	Access to Clearswift product and Operating System updates: **products.clearswift.net** **rh7-repo.clearswift.net**
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 Clearswift ARgon for Email 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)
9090	TCP	In/Out	Connection to Red Hat Cockpit
11371	TCP	In/Out	HTTPS Key Server Queries
19200	UDP	In/Out	Broadcasting of greylisting data to Peer Servers

Appendix E: Password policy

The default password policy applied after the ARgon for Email installation uses specific rules from the DISA STIG security profile. This is the same for all installation methods. For non-ISO installs, extra steps will still need to be followed in order to apply the rest of DISA STIG profile if required. See Appendix F for further details

Policy	Required
The minimum number of required classes of characters for the new password (uppercase, lowercase, digits, non-alphanumeric characters)	4
The minimum acceptable size for the new password	15
The minimum number of upper case characters in the password	1
The minimum number of lower case characters in the password	1
The minimum number of digits in the password	1
The minimum number of non-alphanumeric characters in the password	1
The maximum number of allowed consecutive characters of the same class in the new password	4
The maximum number of allowed consecutive same characters in the new password	3
The maximum number of characters in the new password that can be reused from the old password	8
Prevent use of dictionary words	true

> (i) Refer to your organization's own best practices and recommendations when creating suitable passwords that meet Clearswift's password policy.

Appendix F: How to apply the 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.

> ⚠ Before applying this security profile, please be aware that the performance of traffic-processing on your ARgon for Email could be reduced.
>
> This is due to the increase in the level of auditing performed by the Red Hat audit service. Clearswift recommends that you carefully monitor performance before and after applying the profile, and assign additional hardware resources if required.

Installing via the ARgon for Email ISO

If you have installed your ARgon for Email using the ISO Image, the DISA STIG security profile is automatically applied for Red Hat 7.8. This is implemented using Open Security Content Automation Protocol (OSCAP).

Installing via the Software install process

For the Software install process, you will need to apply the DISA STIG security profile to your Red Hat 7.8 Server both before and after ARgon for Email has been installed.

Upgrading a previous ARgon for Email

If you upgraded from a previous version of ARgon for Email, follow these instructions to apply the DISA STIG security profile:

For the Upgrade process, you only need to apply the profile after the upgrade has completed. See Applying profile after the ARgon for Email installation.

Applying profile before the ARgon for Email installation

The following steps will apply the security profile to your server before you install ARgon for Email using the Software install process.

1. Open the terminal on your Red Hat 7.8 server.

2. Login as the root user.

3. Install the following packages:

```
yum -y install scap-security-guide
```

4. Execute this command to apply the security profile:

```
oscap xccdf eval --remediate --profile xccdf_org.ss-
gproject.content_profile_stig --report /tmp/disa-stig-
report.html /usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
```

5. You can check the level of compliance that has been applied by viewing /tmp/disa-stig-report.html.

6. Reboot the system in order for the DISA STIG security profile modifications to be applied.

Applying profile after the ARgon for Email installation

The following steps will re-apply the security profile to your server after installing ARgon for Email.

1. If you have not enabled online repositories, insert your ARgon for Email ISO.

2. Enter the following URL into a supported web browser to load the Cockpit administration user interface:

   https://<ip-address>:9090

3. Log in to Cockpit using the credentials for your administrator account, ensuring the **Reuse my password for privileged tasks** option is selected.

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.

Evaluating ARgon for Email

To evaluate the DISA STIG Compliancy rating of your ARgon for Email, you can generate a report by following these instructions:

1. Enter the following URL into a supported web browser to load the Cockpit administration user interface:

   https://<ip-address>:9090

2. Log in to Cockpit using the credentials for your administrator account, ensuring the **Reuse my password for privileged tasks** option is selected.

3. Navigate to **Terminal**. Assume root user privileges using the following command:

```
sudo su
```

4. Execute the following script:

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

5. The report will be available from:

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

> Customers wishing to validate their DISA STIG compliance can do so by contacting Clearswift customer support and requesting a compliance document.