

ARgon for Email

Installation & Getting Started Guide

Version 5.0.0

Document Revision 1.0

Copyright

Revision 1.0, September, 2020

Published by Clearswift Ltd.

© 1995-2020 Clearswift Ltd.

All rights reserved. The intellectual property rights in the materials are the property of Clearswift Ltd and/or its licensors. The materials may not be reproduced or disseminated or transmitted in any form or by any means electronic, mechanical, photocopying, recording, or otherwise stored in any retrievable system or otherwise used in any manner whatsoever, in part or in whole, without the express permission of Clearswift Ltd.

The Clearswift Logo and Clearswift product names are trademarks of Clearswift Ltd. All other trademarks are the property of their respective owners. Clearswift Ltd. (registered number 3367495) is registered in Britain with registered offices at 1310 Waterside, Arlington Business Park, Theale, Reading, Berkshire RG7 4SA, England. Users should ensure that they comply with all national legislation regarding the export, import, and use of cryptography.

Clearswift reserves the right to change any part of this document at any time.

Click [here](#) to read Copyright, Trademark, and third party acknowledgments in full.

Contents

Copyright	ii
Contents	iii
1. About this guide	5
1.1 Who is this guide for?	5
1.2 What is Clearswift ARgon For Email?	5
2. Before installing	6
2.1 Types of installation	6
2.2 Obtaining the software	6
2.3 Prerequisites	6
2.3.1 Hardware requirements	6
2.3.2 Installation media	7
2.3.3 Browser support	7
3. Installing Clearswift ARgon For Email	8
3.1 Installing Red Hat 7.8 and ARgon For Email from the ISO image	8
3.2 Starting The Installation	9
3.3 Configuring the ARgon Server	10
3.4 Creating Administrator Accounts	11
3.5 Configuring Update Repositories	12
4. Upgrading From ARgon Server 4.x	13
4.1 Preparing to Upgrade	13
4.2 Unsupported Environments	13
4.3 Checking Prerequisites	13
4.4 Upgrading the ARgon Server	16
4.5 Post-Upgrade Actions	17
4.5.1 Create new Administrator Account(s)	17
4.5.2 Applying the DISA STIG security profile	17
4.5.3 Future Updates	17
Appendix A: Software install process	19
Installing from ARgon Server ISO	19
Installing from Clearswift Online Repositories	20
Post installation considerations	21
Installing additional software	22

Appendix B: Resolving upgrade failures	23
ARgon Server does not meet Red Hat 7.8 pre-requisites	23
Importing ARgon Server 4.x Backup to ARgon Server 5.x	23
Appendix C: USB installation media preparation	24
Appendix D: Firewall ports	26
Appendix E: Password policy	28
Appendix F: How to apply the DISA STIG security profile	29
Installing via the ARgon Server ISO	29
Installing via the Software install process	29
Upgrading a previous ARgon Server	29
Applying Profile before the ARgon Server Installation	29
Applying Profile after the ARgon Server Installation	30
Evaluating the ARgon Server	30

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.

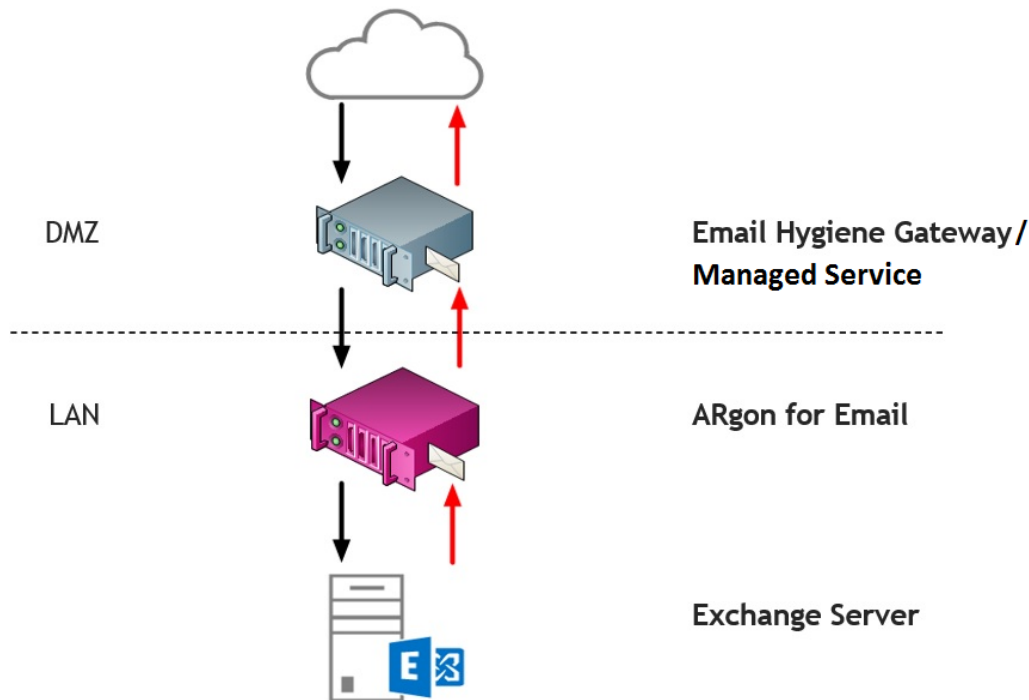
1.1 Who is this guide for?

This guide is intended for use by:

- New customers installing the Clearswift ARgon For Email for the first time.
 - Existing customers upgrading from an earlier version 4 release of the Clearswift ARgon For Email to version 5.0.0.
-

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. The ARgon Server 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 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 above platform.	Appendix A: Software Install Process
Packaged Hardware Platform	Applies to users deploying the product using pre-installed hardware supplied by Clearswift.	Configuring the Gateway

2.2 Obtaining the software

You can obtain the Clearswift ARgon For Email software from:

- The [Clearswift download area](#) where you can download the Clearswift ARgon For Email ISO image.
- Clearswift, with your pre-installed hardware.

2.3 Prerequisites

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

2.3.1 Hardware requirements

Your computer or virtual machine requires a minimum of 6 GB RAM and a 60 GB hard drive for use in testing and demonstration environments.

Clearswift recommends a minimum of 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 Server is configured so that your policy has:

- Optical Character Recognition 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 Spec	Under 20,000 msgs/hour	2	10	200+	Optional
Virtual - High Spec	75,000 msgs/hour	4	16	300+	Yes



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

2.3.2 Installation media

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

- EMAIL-5.0.0.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.

2.3.3 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)

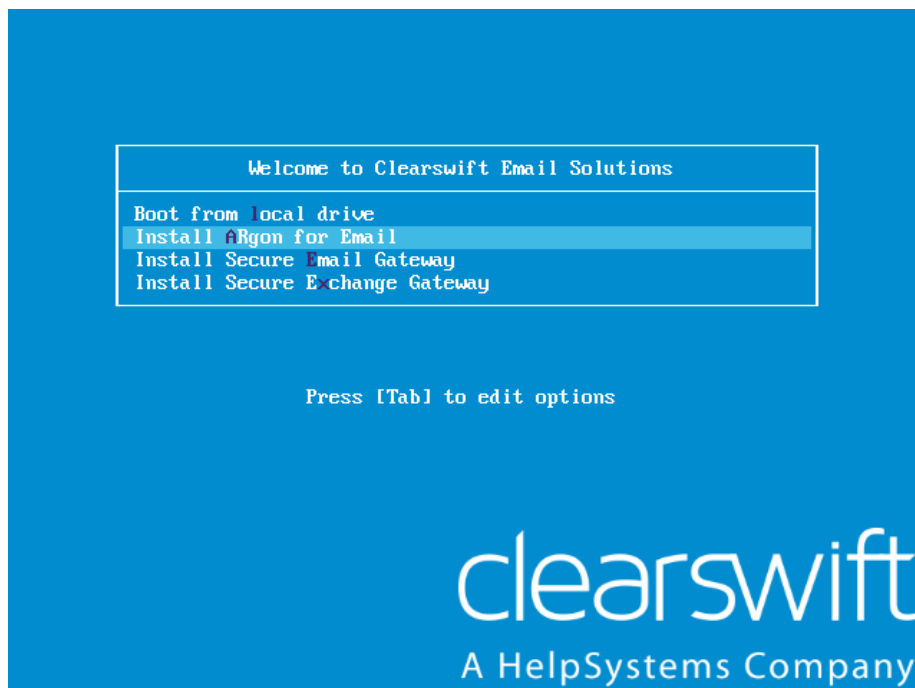
3. Installing Clearswift ARgon For Email


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.



We *strongly recommend* configuring each network card with a static IPv4 network address.

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



Warning! 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 is required because post-installation you are *strongly advised* to disable the root user account as a security precaution.
 - This can also be done post-installation via the Red Hat Cockpit application.
 - It is good practice to create a backup administrator user in case the primary administrator password is lost.

4. The package installation takes approximately 15-20 minutes to complete.
 - Once complete, the Red Hat Installation Wizard automatically reboots.

3.3 Configuring the ARgon Server

On restart, you will need to complete the Clearswift ARgon For Email Installation wizard.

1. Open a supported Web browser and navigate to the Gateway IP address:
<https://<ip-address>/Appliance>
2. The Gateway Installation Wizard is displayed.

ARgon for Email

clearswift
A HelpSystems Company

Thank you for choosing **Clearswift**. The setup process consists of a few easy steps, during which you will be asked to provide information on your network configuration.

You will have been supplied with a license key and serial number by your supplier. Please enter these details now.

Company Name :

License Key :

Serial Number :

Next

Copyright © HelpSystems, LLC (5_0_0_202008061113)



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

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 Gateway interface is accessible.

3.4 Creating Administrator Accounts

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

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

This can be achieved using the Red Hat Cockpit application.

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 **Re-use my password for privileged tasks** is checked.



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. Select **Accounts** and click **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**. Then select 'Never lock account' and click **Change**.
 - Select **Never expire password** or the **date** on which the password will expire. Then click **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 'Re-use my password for privileged tasks' setting.

6. Select Accounts and click the root user.
 - Select the **Lock Account** setting 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 Server releases.

Alternatively, if the ARgon Server 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. 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.

Online repositories can be enabled by following the steps below:



Be aware that enabling online repositories is an irreversible action.

1. Enter the Cockpit URL into a supported web browser to load the Cockpit Administration User Interface. Then login using the administrator credentials, ensuring that you have selected the **Re-use my password for privileged tasks** setting.
2. Select Clearswift and then under **Product Actions**, click **Enable** in the Enable online repositories setting.

4. Upgrading From ARgon Server 4.x



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

4.1 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.

4.2 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 Clearswift ARgon For Email software on one of these, refer to [Appendix B: Resolving Upgrade Failures](#) for further information.

4.3 Checking Prerequisites



4.11.2 is minimum version required to upgrade to ARgon For Email 5.0.

You will also need to download a copy of the version 5.0 ISO to complete an upgrade from 4.11.2. See [Prerequisites](#) for more information.

To upgrade your ARgon Server to ARgon For Email 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.
- Please ensure you follow the upgrade instructions in the ARgon For Email [4.11.2 Installation Guide](#) so that your ARgon Server is correctly configured before attempting to upgrade to version 5.0.0.

On completion of the 4.11.2 upgrade, you will be ready to upgrade to Red Hat 7.8 and ARgon For Email 5.0.0.

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 v5.0.0 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 the 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. Please do not restart your ARgon Server 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 Server not meeting the necessary pre-requisites to be upgraded, please refer to [Appendix B: Resolving Upgrade Failures](#).

4.4 Upgrading the ARgon Server

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 the Red Hat Cockpit application and create new administrator account(s) that you will then use to administer the ARgon Server 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 the ARgon Server from an ARgon For Email 4.x Terminal Session is no longer available in ARgon For Email 5.0.

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.



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. To check on the progress of the upgrade, enter the following command and follow the

instructions provided:

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

4.5 Post-Upgrade Actions

The Red Hat and ARgon server 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.

4.5.1 Create new Administrator Account(s)

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

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

See [Creating Administration Accounts](#) for further information on creating new accounts.



The cs-admin user account previously used in Gateway 4.x is not supported. You must use a new Administrator Account instead.

4.5.2 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.

4.5.3 Future Updates

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

1. Enter the following URL into a supported web browser to load the Cockpit Administration UI:

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

2. Select '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).



You should install Red Hat 7.8 as a **Minimal** server installation, with a separate `/`(root) and `/var` partition. The root partition should be 20GB (minimum) and `/var` should use a minimum of 60 GB for test environments and 200GB for production environments.



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 Server installation. See [Appendix F](#) for details.

Installing from ARgon Server 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 Clearswift 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-gateway-repo cs-rhel7-mirrors
```

6. Install the required product using the following command:

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



If 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 the ARgon Server](#).

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.



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 the link below to open a page from where the commands can be individually copied and pasted into your terminal:

```
curl -Of https://-  
products.clearswift.net/gw/5.0.0/platform/cs-rhel7-mirrors-  
20.06.02-200714105620.x86_64.rpm  
  
curl -Of https://products.clearswift.net/gw/5.0.0/gw/cs-gate-  
way-repo-5.0.0.rpm
```

3. Download and install the Clearswift GPG public key:

```
rpm --import https://products.clearswift.net/it-pub.key
```

4. Verify the downloaded packages:

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

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

```
cs-gateway-repo-5.0.0.rpm:  
  
Header V5 RSA/SHA1 signature, key ID 5522142c: OK  
Header SHA1 digest: OK (2177181a2b83543fd34437ca4c97aff4dc04e967)
```

```
V5 RSA/SHA1 Signature, key ID 5522142c: OK
MD5 digest: OK (03b7bca68386808665d164a7ee39f47e)
```

```
cs-rhel7-mirrors-20.06.02-200714105620.x86_64.rpm:
```

```
Header V4 RSA/SHA1 signature, key ID 5522142c: OK
Header SHA1 digest: OK (ad89b88e74b85a9408007cd5403dc3381dbc515e)
V4 RSA/SHA1 Signature, key ID 5522142c: OK
MD5 digest: OK (d81d13c9c509db0b60c21aba8a72c5fe)
```

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 the ARgon Server.



If 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 the ARgon Server](#).

Post installation considerations

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

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



You should avoid changing network configuration at the command line as the ARgon Server 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 Server 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 Clearswift 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.



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 Server using the instructions in section 4: [Upgrading from ARgon Server 4.x](#), the following sections provide you with some options on how to upgrade or migrate your existing Gateway policy.

ARgon Server does not meet Red Hat 7.8 pre-requisites

If the upgrade failed because your ARgon Server 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.

Importing ARgon Server 4.x Backup to ARgon Server 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 Server 5.x server and then import a ARgon Server 4.x backup.



Importing a ARgon Server 4.x backup does not automatically restore the peer group roles so they must be restored manually.



See [Backup and Restore the system](#) in 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](#).



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. Please ensure it is the portable version.



Although you can use USB tools other than Rufus, the following USB tools will not work with the Clearswift 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_GW_RHEL.

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 data 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 you are using PMM)
80	TCP	Out	Access to Clearswift product and Operating System updates at repo.clearswift.net and rh.repo.clearswift.net
80	TCP	Out	HTTP access to the ARgon Server 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 the ARgon Server
162	UDP	Out	SNMP alerts
389	TCP	In/Out	LDAP directory access (if you use LDAP servers beyond the firewall)

Port	Protocol	Direction	Required for
389	TCP	In/Out	LDAP Key Server Queries
443	TCP	In/Out	HTTPS access to the 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	In/Out	HTTPS Key Server Queries
514	TCP	Out	Access to the central SYSLOG server (log export)
636	TCP	In/Out	Secure LDAP/S directory access
990	FTPS	In/Out	Backup & Restore and Transaction Logging. Also used to connect the ARgon Server 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 ARgon Server 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



Please 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 Gateway 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 Server ISO

If you have installed your ARgon Server 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 the ARgon Server has been installed.

Upgrading a previous ARgon Server

If you upgraded from a previous version of the ARgon Server, 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 Server Installation](#).

Applying Profile before the ARgon Server Installation

The following steps will apply the security profile to your server before you install the ARgon Server 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.ssgproject.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 Server Installation

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

1. If you have not enabled online repositories, insert your ARgon Server ISO.
2. Open a supported Web browser and open Cockpit:
<https://<gateway-ip-address>:9090>
3. Log in using your administrator account details and ticking the **Reuse my password for privileged tasks** option.
4. Click **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 the ARgon Server

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

1. Open a supported Web browser and open Cockpit:
<https://<gateway-ip-address>:9090>
2. Log in using your administrator account details and ticking the Reuse my password for privileged tasks option.
3. Click Terminal.
4. Assume root user privileges using the following command

```
sudo su
```

5. Execute the following script

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

6. 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.