clearswift

Frequently Asked Questions (FAQ)

Clearswift SECURE Email Gateway 4.6

Issue 1.0

March 2017

Copyright

Version 1.0, March 2017

Published by Clearswift Ltd.

Contents

What's new in V4.6

This new release brings additional security features to the Clearswift SECURE Email Gateway.

The 4.6 release has the following new features:

- Phishing detection
- Message Sanitization
- DMARC
- Malware Outbreak detection
- DKIM improvements
- Support for Azure

Can I upgrade to 4.6 from 3.8.x?

There is no in-place upgrade mechanism, but customers are advised to install 4.6 onto a fresh system and then restore the configuration from their 3.8.* system. This will copy their existing policy but not any local networking options such as hosts files or static routes.

Can I install 4.6 directly?

New customers can install 4.6 directly, there is no need to install 4.0 / 4.1 / 4.2 or 4.3 first.

How do I upgrade from 4.x to 4.6?

The instructions are listed in the Installation and Setup Guide, but here they are:

1. Enable online repositories
    a. Open an SSH session and access the Clearswift Server Console. Log in using your default cs-admin access credentials.

    b. Use the arrow keys and the **OK** button to select:
    Configure System > **Select YUM repositories** > **Enable online Repositories**

2. Download software updates
    a. From the Clearswift Server Console main menu, select:
    Configure System > **View and Apply Software Updates**> **Download New Updates** > **OK**

    b. The console displays a progress bar indicating the status of the download. Click **OK** when the download is complete.

3. Apply software updates
    a. From the Clearswift Server Console main menu, select:

Configure System > **View and Apply Software Updates** > **Apply Updates** > **OK**

b. Confirm that you want to apply the updates by clicking **Yes**.
The downloaded system updates and product updates are installed.

4. Reboot your system
   a. From the Clearswift Server Console main menu, select:
   Reboot or Shutdown Server > **Reboot** > **OK**

What URL RBL will be used for the URL blacklisting?

The URL RBL is supplied by Clearswift and is currently fixed. It has been requested to support others such as Spamhaus and McAfee.

Can I add my own URLs to be sanitized?

Yes, the system supports customer defined good and bad lists. Bad lists would contain URL's to be sanitized whereas good lists would be for URL's that must be preserved.

Can that URL import be automated on a schedule?

Manual lists are currently updated via the UI only at this point

Is the url filtering in the base license included?

Yes, this is provided at no extra charge to the customer

Are there any Greylisting improvements between 4.5.1 and 4.6?

No.

With the realtime feed - are both Kaspersky and Sophos included?

Kaspersky and Sophos are included based on the product license you may have. The Phishing detection feed is included as standard.

Are there any improvements with ImageLogic?

There has been no changes to ImageLogic in this release.

Do you still need to create DKIM private key manually?

Yes it is still done via the System Console using the command

```
openssl genrsa -out <private.key> 1024
```

Is there a DKIM test on the appliance to verify published DNS Records?

No there is not.

How are you being fed information on your url blacklists to deal with zero day threats?

The gateways don't get a download, they actively check on each message processed via a DNS lookup

Are the existing feature requests migrated to the new "ideas"?

No, there are a lot of enhancements already in the system accumulated over a number of years. We wanted to start this new system fresh so that we are seeing what customers need **now**, and not based on what customers were expecting 5 years ago.

Any chance new encryption features will follow with further updates?

Yes, we have a very active development stream of enhancements to make across the whole product, including encryption.

Any plans to automatically whitelist the recipient addresses of outgoing emails (or to influence the score when a reply email comes in)?

Currently there are no plans for this, but it is something that has been considered in the past.

Are there any plans to allow emails released from PMM to be scanned again by AV in case they were delivered before a relevant update?

Currently there are no plans for this, but it is something that has been considered.

Any plans to support a feature like automatic uploading of large outgoing email attachments to a web portal (maybe via an outlook plugin) so that the recipient can download it from the

web portal (he would then receive an URL instead of the attachment)?

Currently there are no plans for this, but it is something that has been considered.

Have you added the ability to add multiple IP address against one domain as opposed to adding the same domain multiple times with a different IP address

Not in this release.

Will there be new documentation to assist installations in Azure?

Yes, there will be a new document available on the Clearswift website and customer/partner portals.

Is it possible to re-direct to a new url rather than modifying a url with a hash?

Not in this initial release. We will take customer feedback and product performance and evaluate this enhancement.

Does DMARC / DKIM apply to messages from IP addresses on Allowed Relay list?

No, messages from these sources are exempt unless you have selected to scan outbound messages for spam.

You mentioned a Dual Nic fix, was that specifically in regards to Azure ?

The reference to Dual Nic's and Azure is related to the additional steps that have to be performed in order to create a 2nd NIC on an Azure virtual platform to allow features like PMM to work properly.

The current release overwrites custom route files when upgrading. Has this been addressed?

No, that fix is currently scheduled for a release later this year.

Is DANE is something that will be possible with 4.7 or later?

DANE will certainly not feature in 4.7, but it maybe something that we decide to support in a future release. As the 4.7 release will deliver a Postfix MTA to replace

the Sendmail MTA, the ability to use DANE is simplified as Postfix has built-in support for it.

Will the feature scan URLs in attachments too?

No. If you want to look for URL's in attachments you will need to use Detect Lexical Expression

Is message sanitization included in standard SEG license? What about document sanitization how is it related?

Message sanitization is included in the base product, Document Sanitization is a separate chargeable add-on that removes meta-data and change tracking from Documents prior to being delivered.

Can you define the custom lists addresses that contain wildcards?

Yes, its possible to remove/block based on a wildcard URL in the custom list

Do all URLs have to be http or https?

No, its possible to remove/block on url's such as ftp://ftp.clearswift.com

Is there a URL feedback mechanism from each gateway to help protect other customers' gateways?

Currently there is no immediate mechanism for this, and if there was we'd require you to accept a data sharing agreement. Any messages that are not detected will can be fed back to spam@clearswift.com for analysis which could result in the URL being added to the feed.

Are there any best practises for upgrading in a peer network?

As with all forms of system upgrade we recommend you've read the installation notes and readme documents, tested the product and backed up the system.

In a simple configuration of 2 peers, we would recommend to upgrade the machine that is typically used as the peer node that you typically connect to and make changes and run the upgrade from that one first, and if successful then move onto the second node.

In a more complex environment with say 3 processing peers and a separate PMM server, we would suggest starting with the peer that is normally used to manage policy from and if that's successful, then we would suggest the PMM server node next and the remaining 2 peer nodes

Do you have more detail on the file processing bug fixes, particularly PDFs?

There have been a number of issues fixed that should reduce the number of PDF's that fail to process particularly with an "unknown binary" reason and "Dictionary is not font dictionary". Other issues were found with BIFF files (images inside Excel) and some CDA files.

In 4.7 there will be a new Content Rule that will allow customers to override issues with specific formats.

Is the PDF Parsing problem "Failed to parse the XMP document" solved?

Some fixes (as listed before) where "unknown binary" were detected can manifest themselves as an issue in XMP (eXtensible Metadata Platform – is used for the creation, processing and interchange of standardized and custom metadata for digital documents) and should hopefully be improved.