clearswift

Frequently Asked Questions (FAQ)

Clearswift SECURE Email Gateway 4.5

Issue 1.0

October 2016

Copyright

Version 1.0, October, 2016

Published by Clearswift Ltd.

Contents

What's new in V4.5

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

The 4.5 release has the following new features:

- Branding
- AV Heuristics and Behavioral
- External Program
- Spoofing enhancements
- LDAP/S and HTTP/S key server lookups
- MSW Route selection
- Message Reprocessing enhancements

Can I upgrade to 4.5 from 3.8.x?

There is no in-place upgrade mechanism, but customers are advised to install 4.5 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 4.5 directly?

New customers can install 4.5 directly, there is no need to install 4.0 / 4.1 / 4.2 or 4.3 first.

How do I upgrade from 4.1 to 4.5?

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**

Do the AV cloud compromise security?

No, the gateways only transmit hashes of files to be scanned and never the file itself.

Why would I disable the AV Cloud lookups?

If customers were running a "closed network" configuration (where the SEG does not have access to the internet) or in an environment where network latency through multiple upstream proxies would impact processing performance.

Is it possible for the AV heuristic and behavioural scanners to generate FP's?

Yes it is possible, but very unlikely. However given that over 10m samples of new malware are created each month it is always better to be safer than sorry.

Does having these features mean that I don't need a Sandbox?

The heuristics and behavioural methods will help you detect more malware than standard, but they are not a replacement to Sandboxing. Of course Sandbox technologies are expensive and can cause delays in message processing.

When creating an external command what considerations must I observe?

Given that this execution happens in mid process you should consider only running it against relevant format types. For example if you wanted to write a tool to look at a message and look at the message headers and perform some test on the messages routing. In this case it would be sensible to only can the SMTP message container.

The actual execution files must reside on the local filesystem and not a remote system. Configuration of the tool does verify the file must exist before proceeding.

File and group membership must be correctly configured with the file owner as gw-services and group as cs-adm, and file locations read from or written to must be appropriate for this user account.

Finally the time a process takes to perform its operation will also have an impact on message throughput. Ideally, unless message volume is very low you should aim to ensure execution times are less than 10 secs, if message processing exceeds 30 seconds then you might start to see messages being naturally terminated by the processing monitors.

Could I use this feature to check the file in with an external Sandbox?

The answer is "Yes" and "No". So you could take the file extracted from the message and pass that to a Sandbox for verification. However you could not wait for the Sandbox to give you an answer as that is likely to be several minutes. But there is benefit in using the Sandbox to see if the file does indeed contain something dangerous.

I'm still getting spoofed message through?

Yes it is possible for this to happen. Checking has been tightened up, but doesn't close every loophole. In version 4.6 due in February there will be more methods to help to reduce the risks from phishing.

I'm not sure I understand what the changes have been made in route selection?

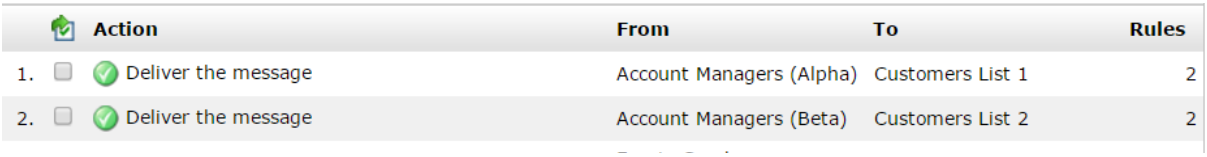
Imagine if you have 2 internal teams of employees who work as account managers for a number of customers. Each account team should only be allowed to mail their own customers, but not the other team's accounts. In both cases the policy rules to be applied are the same.

If you created a policy like this

	Action	From	To	Rules
1.	Deliver the message	Account Managers (Alpha) Account Managers (Beta)	Customers List 1 Customers List 2	2

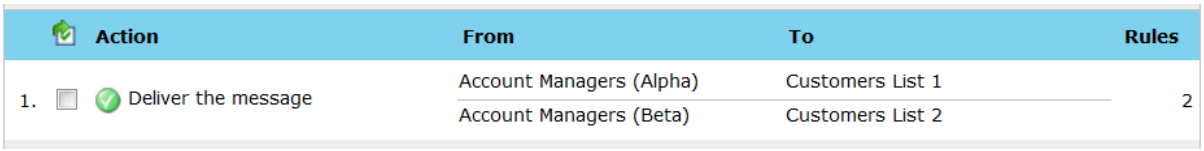
Then both internal teams could mail to any of the customers.

So you would need to create 2 Policy Routes



	Action	From	To	Rules
1.	Deliver the message	Account Managers (Alpha)	Customers List 1	2
2.	Deliver the message	Account Managers (Beta)	Customers List 2	2

In V4.5 it is now possible to create routes within routes to provide the separation of address lists without the overhead of creating an excess of policy routes.



	Action	From	To	Rules
1.	Deliver the message	Account Managers (Alpha) Account Managers (Beta)	Customers List 1 Customers List 2	2

What is the point of the reprocess feature?

If a message has been blocked due to a incorrect policy setting, the System Administrator can make the policy change (to make sure it doesn't happen again) and then they can use the reprocess feature to test the change.