

## Frequently Asked Questions

---

Clearswift SECURE Email Gateway 4.7

November 2017

## Copyright

Published by Clearswift Ltd.

© 1995–2017 Clearswift Ltd.

All rights reserved.

The materials contained herein are the sole property of Clearswift Ltd unless otherwise stated. The property of Clearswift 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.

Information in this document may contain references to fictional persons, companies, products and events for illustrative purposes. Any similarities to real persons, companies, products and events are coincidental and Clearswift shall not be liable for any loss suffered as a result of such similarities.

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.

## Contents

|  |   |
|--|---|
| Overview.....  | 4 |
| Is the jpg removal of meta data part of the redaction license or the ImageLogic?.....  | 4 |
| Is there an option to remote appended data, especially in JPEG files? .....  | 4 |
| Is it possible to get a list of STIG changes in this release so we can compare with changes we may have already made before release? .....   | 4 |
| How do you get the STIG report? .....  | 5 |
| We have used dummy internal MX records rather than A with Postfix in the past. Will this be supported? .....   | 6 |
| We are using more than TLS domain connection. Will we have any support us to prepare the migration?.....   | 6 |
| What about the reporting? Will we be able to customize the report? .....   | 8 |
| In the SWG are there any plans to include support for web sockets in future releases? .....  | 8 |
| In a recent windows updates had a fix for a bug where a malware was embedded in a font , is SEG able to block malware in fonts generally via the file detection engine or does the SEG only rely on the AV Engines?..... | 9 |
| What is a SIEM system? .....   | 9 |
| Was an SELinux policy created for the application? A couple STIG checks fail because that is missing so I'm wondering if that is handled in 4.7 or if that's coming later?.....  | 9 |
| If we already STIG'd the 4.6 version, can we upgrade to 4.7?.....  | 9 |

## Overview

This document lists all common questions and questions asked during the 4.7 live customer webinar sessions.

### Is the jpg removal of meta data part of the redaction license or the ImageLogic?

The meta-data removal is part of the Document Sanitization license, for the redaction of properties in the meta-data that is achieved with the Data Redaction license.

### Is there an option to remote appended data, especially in JPEG files?

That is not available in this release.

### Is it possible to get a list of STIG changes in this release so we can compare with changes we may have already made before release?

The table below lists the applied STIG rules that make up the RedHat *stig-rhel6-server-upstream* profile by default with Gateway 4.7

| Rule ID                                   | Profile |
|---|---------|
| account_disable_post_pw_expiration        | Applied |
| accounts_minimum_age_login_defs           | Applied |
| accounts_password_minlen_login_defs       | Applied |
| accounts_password_pam_dcredit             | Applied |
| accounts_password_pam_difok               | Applied |
| accounts_password_pam_lcredit             | Applied |
| accounts_password_pam_ucredit             | Applied |
| accounts_password_pam_unix_remember       | Applied |
| audit_rules_dac_modification_chmod        | Applied |
| audit_rules_dac_modification_chown        | Applied |
| audit_rules_dac_modification_fchmod       | Applied |
| audit_rules_dac_modification_fchmodat     | Applied |
| audit_rules_dac_modification_fchown       | Applied |
| audit_rules_dac_modification_fchowndat    | Applied |
| audit_rules_dac_modification_fremovexattr | Applied |
| audit_rules_dac_modification_fsetxattr    | Applied |
| audit_rules_dac_modification_lchown       | Applied |
| audit_rules_dac_modification_lremovexattr | Applied |
| audit_rules_dac_modification_lsetxattr    | Applied |
| audit_rules_dac_modification_removexattr  | Applied |

|   |         |
|---|---------|
| audit_rules_dac_modification_setxattr           | Applied |
| audit_rules_mac_modification                    | Applied |
| audit_rules_media_export                        | Applied |
| audit_rules_networkconfig_modification          | Applied |
| audit_rules_time_adjtimex                       | Applied |
| audit_rules_time_clock_settime                  | Applied |
| audit_rules_time_settimeofday                   | Applied |
| audit_rules_time_stime                          | Applied |
| audit_rules_time_watch_localtime                | Applied |
| audit_rules_unsuccessful_file_modification      | Applied |
| audit_rules_usergroup_modification              | Applied |
| bootloader_audit_argument                       | Applied |
| disable_interactive_boot                        | Applied |
| disable_users_coredumps                         | Applied |
| display_login_attempts                          | Applied |
| gconf_gnome_screensaver_idle_activation_enabled | Applied |
| gconf_gnome_screensaver_idle_delay              | Applied |
| gconf_gnome_screensaver_lock_enabled            | Applied |
| gconf_gnome_screensaver_mode_blank              | Applied |
| kernel_module_bluetooth_disabled                | Applied |
| kernel_module_dccp_disabled                     | Applied |
| no_empty_passwords                              | Applied |
| package_aide_installed                          | Applied |
| package_openswan_installed                      | Applied |
| package_screen_installed                        | Applied |
| securetty_root_login_console_only               | Applied |
| service_ntpd_enabled                            | Applied |
| service_rhnsd_disabled                          | Applied |
| sysctl_kernel_exec_shield                       | Applied |
| sysctl_kernel_randomize_va_space                | Applied |

## How do you get the STIG report?

In this version you would need to go in via the console, using the cs-admin account.

Access via the "Open Terminal Session" and navigate to

`/opt/csrh/stig/reports/`

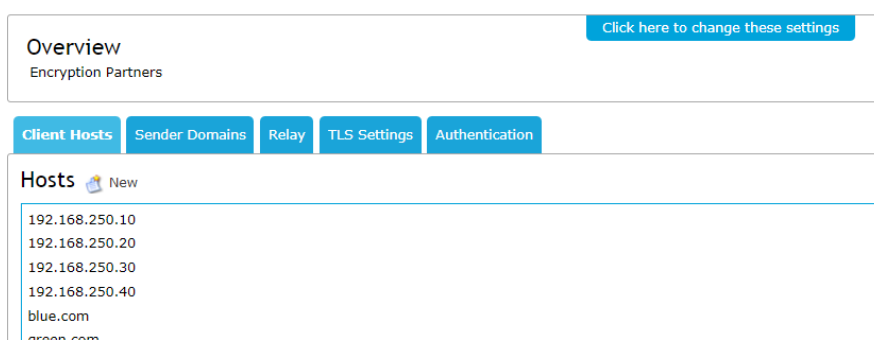
The file cs-remediation-report.html contains the report and can be copied off the system (using FTP)

## We have used dummy internal MX records rather than A with Postfix in the past. Will this be supported?

The SMTP routing table now only supports one routing rule pre domain. It is possible to use a DNS name resolving to multiple host records or to use an internal MX record to route internal mail.

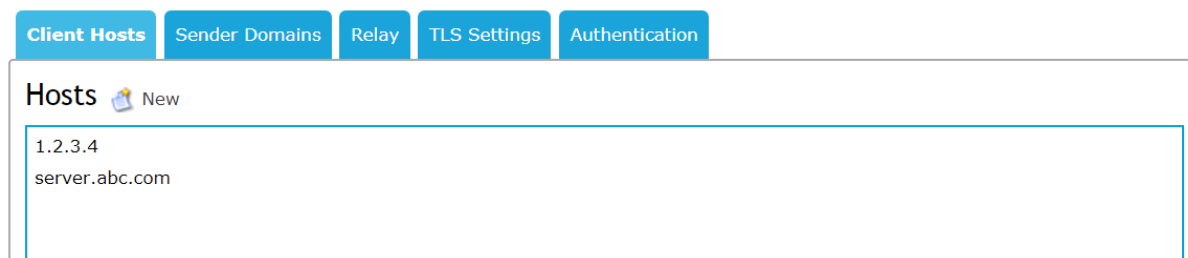
## We are using more than TLS domain connection. Will we have any support us to prepare the migration?

The Gateway upgrade will convert existing policy as best it can. However as Postfix does things differently to Sendmail for inbound mandatory TLS, we need to differentiate between domain names and fully qualified host names, so we have introduced a new tab in the Connections panel so that future Connection configurations can be configured appropriately.




When the upgrade takes place, entries from the Hosts panel in a client connection (that isn't an IP address) will be copied to the new Sender Domains tab.


At this point the SysAdmin needs to ensure that no domain names exist in the Client Hosts.



Only domain names should exist in the domain tab

Client Hosts **Sender Domains** Relay TLS Settings Authentication

**Domains**  New

 You can select Inbound TLS configuration for a Sender Domain only if the connection does not match another Connection Profile by host/IP and if you have Opportunistic TLS enabled.  
A match on Sender Domains does not select configuration for Relay or Authentication.

abc.com

Finally ensure that the inbound mandatory TLS option is enabled

Client Hosts Sender Domains Relay **TLS Settings** Authentication

**Outbound (When Acting as a Client)** [Click here to change these settings](#)

Mandatory TLS for this connection profile is disabled

**Inbound (When Acting as a Server)**

Use Mandatory TLS for this connection profile

**Encryption strength**  
Encryption should meet or exceed :  bits

Outbound Mandatory TLS is also subtly different now. Previously outbound TLS connections were based on the domain name in the client's panel of the connection. With 4.7 you can now define a different TLS security profile on a per domain basis, so we now define TLS profiles and assign it to a domain using the SMTP Routing table.

So a connection profile needs to have Mandatory outbound enabled

Client Hosts Sender Domains Relay **TLS Settings** Authentication

**Outbound (When Acting as a Client)** [Click here to change these settings](#)

Mandatory TLS for this connection profile is enabled

**Supported protocols**  
Use global settings (TLS 1.2)

And that connection profile needs to associated to the domain, using the TLS profile selector

## Edit Email Route



Authentication is not enabled.  
Using mandatory TLS from selected connection profile.

Domain :

Route :  Using DNS  
 To a server

Server :

Port :

Use the outbound TLS configuration from this connection profile :

TLS :

(None)

Use these authentication settings for the email server :

Authentication :

(None)

Username :

The Routing table now has 2 new columns and shows whether SMTP AUTH and TLS are enabled for that domain.

Hosted Domains **Email Routing**

New

Showing 1 - 4 of 4

| Domain                                       | Route                             | AUTH | TLS           |
|--|-----------------------------------|------|---------------|
| <input type="checkbox"/> abc.com             | Use DNS mx record                 |      | Mandatory TLS |
| <input type="checkbox"/> clearswift-test.com | To server at '192.168.250.100:25' |      | (None)        |
| <input type="checkbox"/> examplecompany.org  | To server at '192.168.250.100:25' |      | (None)        |
| <input type="checkbox"/> *                   | Use DNS mx record                 |      | (None)        |

## What about the reporting? Will we be able to customize the report?

The format of the STIG report is fixed.

## In the SWG are there any plans to include support for web sockets in future releases?

Currently there are no immediate plans for support for Web Sockets



## In a recent windows updates had a fix for a bug where a malware was embedded in a font , is SEG able to block malware in fonts generally via the file detection engine or does the SEG only rely on the AV Engines?

The SEG does rely on the AV engines for look for specific malware signatures. At the time of writing there were no known samples exploiting the vulnerabilities and as such there are no signatures available.

## What is a SIEM system?

The term *security information event management* (SIEM), was defined by Gartner in 2005,

- the product capabilities of gathering, analyzing and presenting information from network and security devices
- identity and access-management applications
- vulnerability management and policy-compliance tools
- operating-system, database and application logs
- external threat data

Example SIEM products include Splunk, Arcsight, Log Rhythm

## Was an SELinux policy created for the application? A couple STIG checks fail because that is missing so I'm wondering if that is handled in 4.7 or if that's coming later?

In this release we have enabled a number of STIG fixes, there will be more in each subsequent release.

## If we already STIG'd the 4.6 version, can we upgrade to 4.7?

Yes, it is supported.

## Do we with 4.7 have to have an entry in Mail Domains and Routing for mandatory TLS?

Yes, you will need to create an entry for each domain. You don't need to have a unique connection profile for each domain as these can be shared for one or more.

## Can I configure an error email to an admin if a mandatory TLS connection fails for some reasons?

Currently no. Information regarding any TLS issues can be found in the SMTP log