

## Product Information Bulletin

---

Clearswift SECURE ICAP Gateway 4.7

Issue 1.0

Nov 2017

## Contents

- Overview..... 3
- New Features ..... 3
  - GDPR EU Regional (PII) Policies..... 3
  - STIG hardening ..... 4
  - Sanitize and Redact JPEG image properties..... 5
  - Support for MindManager Files..... 6
  - Support for additional network interface controllers (NICs)..... 6
- Enhancement requests ..... 7
- Bug fixes..... 7
- Availability..... 7
- End of life ..... 7
- Platform support..... 7
- Packaging..... 7

## Overview

This new release delivers a number of customer enhancement requests, as well as additional security features for the Clearswift SECURE ICAP Gateway.

The new features are briefly summarized below, and examined in more detail on the following pages.

- GDPR EU Regional (PII) Policies
- STIG hardening
- Sanitize and Redact JPEG image properties
- Support for MindManager Files
- Support for additional network interface controllers (NICs)

## New Features

### GDPR EU Regional (PII) Policies

Key points:	
•	Consistent set of PII tokens to cover Passport, Social Security/ Driving License and National Identity (where applicable)
•	Covering 28 countries

With heavy penalties for Data Loss under the regulations of GDPR coming into force in May 2018 customers need to ensure that Personal Identifiable Information (PII) data is controlled.

	Austria	Belgium	Bulgaria	Croatia	Cyprus	Czech Republic	Denmark	Estonia	Finland	France	Germany	Greece	Hungary	Ireland	Italy	Latvia	Lithuania	Luxembourg	Malta	Netherlands	Poland	Portugal	Romania	Slovakia	Slovenia	Spain	Sweden	UK
Passport	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
Social Security	Yellow	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
Driving License	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
Identity Card	Green	Yellow	Yellow	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green	Green
4.6	Yellow																											
4.7	Green																											

*PII Tokens added in 4.7*

The Clearswift products have been extended to support a much wider range of entries allowing a much greater chance to protect employee and customer data from being lost.

## STIG hardening

### Key points:

- Defined by DISA
- Guidelines for more secure deployments of standard COTS products (operating systems, web servers & databases)
- Automatically applied
- 55 recommendations implemented in 4.7

Ensuring that system security is fully maintained against industry best practice is paramount. The Gateways now include conformance to a number of security recommendations created by the Defense Information Systems Agency (DISA) who have crafted the Security Technical Implementation Guides (STIGs). The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack.

In 4.7 there are 55 recommendations that have been applied, and each Gateway release will contain progressively more.

These security recommendations are automatically applied on installation and upgrade, and customers can view the STIG report by logging into the console and accessing the report here

- `/opt/csrh/stig/reports/cs-remediation-report.html`

The report is in HTML so it is advisable to get the file off the Gateway using FTP/SFTP or similar process

**OpenSCAP Evaluation Report**

Guide to the Secure Configuration of Red Hat Enterprise Linux 6

with profile **Clearswift**  
— Clearswift RHEL8 STIG Profile

This guide presents a catalog of security-relevant configuration settings for Red Hat Enterprise Linux 6. It is a rendering of content structured in the extensible Configuration Checklist Description Format (XCCDF) in order to support security automation. The SCAP content is available in the `scap-security-guide` package which is developed at <http://redhat.com/redhat/errata/rhel8-security-guide>.

Providing system administrators with such guidance informs them how to securely configure systems under their control in a variety of network roles. Policy makers and baseline creators can use this catalog of settings, with its associated references to higher-level security control catalogs, in order to assist them in security baseline creation. This guide is a catalog, not a checklist, and satisfaction of every item is not likely to be possible or sensible in any operational scenario. However, the XCCDF format enables granular selection and adjustment of settings, and their association with OVAL and DCCL content provides an automated checking capability. Transformations of this document, and its associated automated checking content, are capable of providing baselines that meet a diverse set of policy objectives. Some example XCCDF Profiles, which are selections of items that form checklists and can be used as baselines, are available with this guide. They can be processed, in an automated fashion, with tools that support the Security Content Automation Protocol (SCAP). The DISA STIG for Red Hat Enterprise Linux 6, which provides required settings for US Department of Defense systems, is one example of a baseline created from this guidance.

Do not attempt to implement any of the settings in this guide without first testing them in a non-operational environment. The creators of this guidance assume no responsibility whatsoever for its use by other parties, and makes no guarantees, expressed or implied, about its quality, reliability, or any other characteristic.

**Evaluation Characteristics**

Target machine	cs-gw-24026	CPE Platforms	Addresses
Benchmark URL	<a href="http://open.compliance/defintons/scap-rhel8-xccdf_cs.xml">http://open.compliance/defintons/scap-rhel8-xccdf_cs.xml</a>	<ul style="list-style-type: none"> <li>• <a href="#">cpe:/o:redhat:enterprise_linux:6</a></li> <li>• <a href="#">cpe:/o:redhat:enterprise_linux:6:el6</a></li> <li>• <a href="#">cpe:/o:redhat:enterprise_linux:6:el6</a></li> </ul>	<ul style="list-style-type: none"> <li>• <a href="#">127.0.0.1</a></li> <li>• <a href="#">192.168.16.10</a></li> <li>• <a href="#">00:00:00:00:00:00</a></li> <li>• <a href="#">00:00:29:81:9C:22</a></li> </ul>
Profile ID	Clearswift		
Started at	2017-09-10T17:54:02		
Finished at	2017-09-10T17:54:03		
Performed by			

**Compliance and Scoring**

There were no failed or uncertain rules. It seems that no action is necessary.

**Rule results**

55 passed

Severity of failed rules

*Example – STIG report*

In most cases the Sysadmin won't notice any changes but some of the more obvious ones are

- NTP enabled by default on install and upgrade
- Increased auditing of user actions in Console and terminal windows
- New console (not SSH) message prior to login
- New logon message after login prior to the Console loading

## Sanitize and Redact JPEG image properties

### Key points:

- Allows redaction of image properties
- Allows sanitization (removal) of image properties
- Included as part of Data Redaction / Document Sanitization Licenses

Previously the Redaction and Document Sanitization features were limited to Text, Documents, Message bodies and Web Pages; this version allows customers with the appropriate license to inspect image meta data and optionally redact items or remove properties.

This is particularly important to organizations where either

- the exact location where the picture was taken is sensitive
- the time that the picture was taken
- or the device used to take the picture is sensitive

LensMake	Apple
LensModel	iPhone 6s Plus back camera 4.15mm f/2.2
	---- GPS ----
GPSLatitudeRef	North
GPSLatitude	50.618636°
GPSLongitudeRef	West
GPSLongitude	2.249858°
GPSAltitudeRef	Above Sea Level
GPSAltitude	2.83715847 m
GPSTimeStamp	12:02:39
GPSSpeedRef	km/h
GPSSpeed	0
GPSImgDirectionRef	True North
GPSImgDirection	147.6948529
GPSDestBearingRef	True North
GPSDestBearing	147.6948529
GPSDateStamp	2017:05:21
GPSHPositioningError	5 m
	---- IFD1 ----
Compression	JPEG (old-stvle)

*Example – Image meta data showing GPS location where picture was taken*

The Redaction features can redact specific text from the properties, or some or all of the image meta data may be removed.

Workspace	
Tag name	Value
YCbCrSubSampling	YCbCr4:2:0 (2 2)
	---- IFDO ----
Make	Apple
Model	***** 6s Plus
Orientation	Horizontal (normal)
XResolution	72
YResolution	72

*Example – Image properties following redaction of the text "iPhone"*

## Support for MindManager Files

### Key points:

- Support to MindManager files (MMAP format) as media type

SIG supports MindManager files (MMAP format) as a media type on the following content rules:

- Detect media types
- Run external command
- Detect Malformed Data
- Check Registered Data

## Support for additional network interface controllers (NICs)

### Key points:

- Support to more than one IP address on NICs through the Clearswift ICAP Gateway user interface

It is now possible to specify more than one IP address on NICs through the admin user interface.

## Enhancement requests

The following customer reported enhancement requests have been implemented in this release.

ER#	Summary
<a href="#">WEB-7601</a>	Transaction Log Export - SFTP fails with Test and Manual Export
<a href="#">MAIL-11104</a>	Support for Greek, Turkish, and Norwegian Time Zones

## Bug fixes

A number of client-reported bugs have been fixed in this release. Please see the release notes for more information.

## Availability

Phase	Date
General Availability	November 2017

## End of life

This release will signal the start of the SIG 4.5 end of life program. Version 4.5's EOL program will last 12 months (as defined in the Support Services handbook) and will reach end of life on 7<sup>th</sup> November 2018.

## Platform support

Clients with low memory and low disk space systems may find that their hardware is no longer suitable and may need to refresh their hardware / virtual systems.

Clearswift recommends that systems have a minimum of 4 GB RAM, multi-core processors that support 64bit instructions and over 250 Gb+ of disk space for low volume production environments.

For customers with a greater workload the recommended minimum would be 6-8 GB RAM, dual multi-core processors and 250Gb+ of disk storage and SSD.

## Packaging

Clients using 4.0 to 4.6 will be able to upgrade their system through the Admin console.

To make the installation process easier, clients will be able to request professional services from Clearswift to assist in the deployment of this new version.