clearswift
RUAG Cyber Security

Product Information Bulletin

Clearswift SECURE Web Gateway 4.7

Issue 1.0

Nov 2017

Contents

Overview 3
New Features 3
Client Identification Headers 3
HTTP Performance Improvements 4
GDPR EU Regional (PII) Policies 4
STIG hardening 5
Sanitize and Redact JPEG image properties 6
Support for MindManager Files 7
Support for additional network interface controllers (NICs) 7
Enhancement requests 7
Bug fixes 8
Availability 8
Interoperability 8
End of life 8
Platform support 8
Packaging 9

Overview

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

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

- Client Identification Headers
- HTTP Performance Improvements
- 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

Client Identification Headers

Key points:

- Support to Forwarded, X-Forwarded-For and X-Authenticated-User headers
- Gateway can send two types of client identification headers to a upstream proxy

The user authentication data will be forwarded to the upstream proxy. The upstream proxy can be any solutions that supports authentication headers, like cloud apps, firewall, SaaS services, etc.

Gateway can send two types of client identification headers to a upstream proxy:

- HTML headers Forwarded and X-Forwarded-For
  - Disclose the originating IP address of a client to a upstream proxy

- HTML header X-Authenticated-User
  - Disclose the authentication information (domain + username) of a client to a upstream proxy
  - Flexible header format to meet specific customers requirements. Default format is WinNT://%DOMAIN%/%USER%
  - Supports Base64 encoding

HTTP Performance Improvements

Key points:

- Red Hat kernel tuning to improve the number of HTTP concurrent connections
- Initial tests with one AV engine shows at least a 25% scalability increase over the previous release for HTTP traffic

From call home data, on average 52% of customers traffic is HTTP. Adjustments were made to the Red Hat Kernel to provide a better experience and performance for most customers using HTTP protocol. These changes are applied automatically during the new installation or upgrade.

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																												
Social Security																												
Driving License																												
Identity Card																												
4.6																												
4.7																												

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

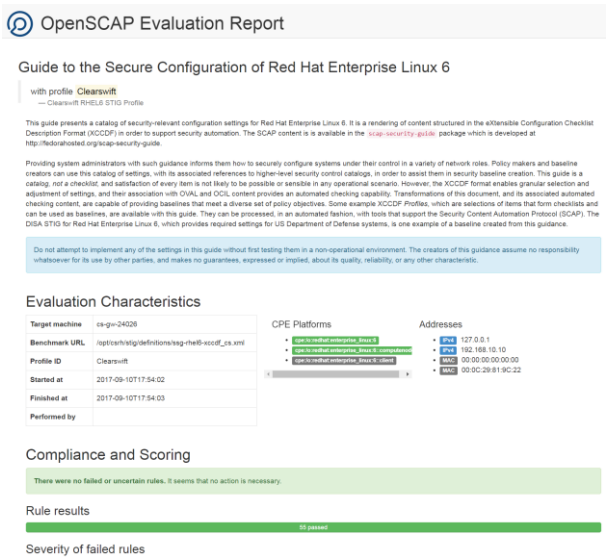
Ensuring that system security is fully maintained against industry best practice is paramount. The Gateways now include conformance to a number of security recommendations created by the Defense Information Systems Agency (DISA) who have crafted the Security Technical Implementation Guides (STIGs). The 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



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

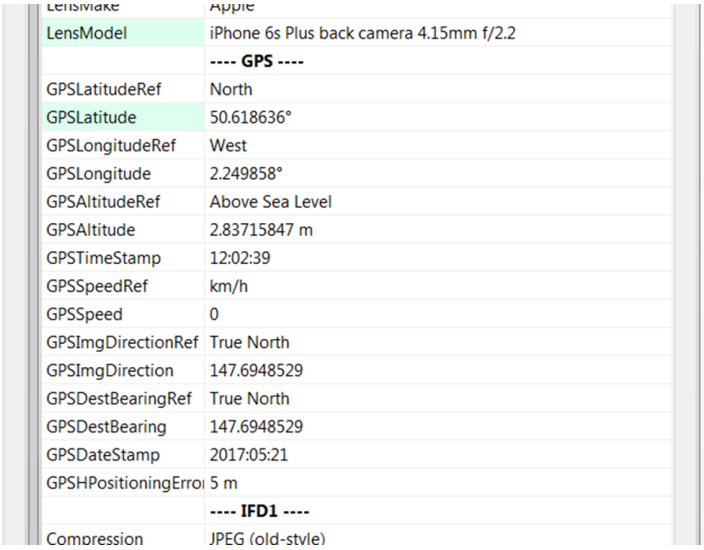
Key points:

- 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

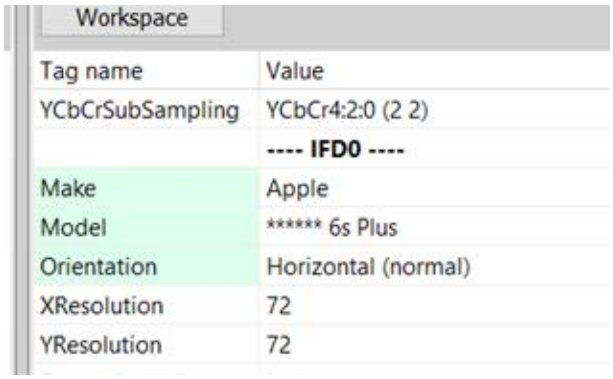
- the exact location where the picture was taken is sensitive
- the time that the picture was taken
- or the device used to take the picture is sensitive



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
GPSHPositioningErro	5 m
	---- IFD1 ----
Compression	JPEG (old-style)

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.



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

Support for MindManager Files

Key points:

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

SWG 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 Web 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
WEB-7601	Transaction Log Export - SFTP fails with Test and Manual Export
MAIL-11104	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

Interoperability

It is possible to peer a Version 4.7 Gateway with an existing Version 3.x Gateway although it will not be possible to share policy due to the different levels of functionality in the later products.

It will be possible to import a 3.8 configuration into a V4.6 system thus saving deploying a V4.0 (or 4.1 to 4.3) and then upgrading that to V4.7.

End of life

This release will signal the start of the SWG 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 7th 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

This release will NOT be available as a patch for all systems running 3.x to automatically download.

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

Clients who want to migrate from 3.x must install a new system and migrate their existing configuration to the new system. They will typically deploy the solution in a test mode initially and then deploy a production system.

Clients will be able to import a V3.8.* policy file to replicate their policy or a V3.8.* full system backup if they want to import reporting data, logs and policy.

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.