Symantec Web Isolation

Version 1.14 Release Notes

August 2020

Copyright

Email: documentation.inbox@broadcom.com

Table of Contents

TABLE OF CONTENTS 3

OVERVIEW 4

WHAT'S NEW IN WEB ISOLATION VERSION 1.14 4

- End User Experience 4
- Security Enhancements 4
- Management Platform Enhancements 4
- Security Policy Granularity 5
- Integration 5
- Miscellaneous 5

UPGRADE INSTRUCTIONS 6

- Supported Source Versions 6
- After Upgrading from Version 1.12 and Earlier 6
- Before and After Upgrading from Version 1.11 and Earlier 7
- Before Upgrading from Version 1.10 7

KNOWN LIMITATIONS 9

- End User Experience 9
- Chrome End Users 9
- Internet Explorer End Users 9
- Safari End Users 9
- Gateway 9
- File Downloads, File Uploads and File Viewer 10
- Management 10

RELATED DOCUMENTATION 10

Overview

This document provides an overview of the changes and enhancements in Symantec Web Isolation 1.14

What's New in Web Isolation Version 1.14

End User Experience

- Browser Notifications
  - Support for browser notifications in isolated sessions
- Timezone is now set automatically in isolated sessions, according to the end-user's timezone
- Localization of end user messages
  - Custom end-user browser messages in isolated sessions, including support for different languages

Security Enhancements

- PAC file security
  - Option to serve the PAC file over standard HTTPS
  - Option to randomize PAC file URL
- Content inspection in proxy mode (Inspect action) now supports file upload policy
- HSM integration
  - Integration with Thales Luna HSM, for signing server certificates when inspecting SSL traffic
- Document isolation support for MPP and MPT file formats

Management Platform Enhancements

- Logging scalability
  - Major improvement in logging & analytics pages load time
- Amazon S3 configuration for activity log forwarding in JSON format
- Log export verbosity level setting
  - Control Activity Logs verbosity level when forwarding logs to Amazon S3 and Kafka
- The management portal is now hosted on https://<mgmt-server-hostname>/console. Access is via port 443. The legacy port 9000 is still supported via https://<mgmt-server-hostname>:9000/
- Automatic log purging to maintain a configurable percentage of free disk space
- Manual deletion of Activity / Audit / Event log index files via the Management portal (limited to super-admin only)
- Monitoring the Management audit logs service from the Management machine

- New license entitlements view

Security Policy Granularity

- Ability to match a rule using destination port criteria
- Selective proxy forwarding policy to an upstream proxy based on hostname or URL
- Enhanced granularity for Selective Isolation in online service suites
    - Option to isolate some, but not all, of the online services included in online service suites
    - Ability to customize the list of suite service URLs

Integration

- Enhanced DLP integration. Session context, including user name, is now shared with the DLP platform, and thus available in DLP reports
- Native SKU integration with Cynic
- MetaDefender Cloud V4 API upgrade
- Google safe browsing is no longer supported

Miscellaneous

- Policy matching performance improvements

Upgrade Instructions

After the Report Server upgrade, past logs are converted to a new format. This is an offline process that takes place after the upgrade and may last several days. During this process, the Report Server continues to generate logs.

Supported Source Versions

The upgrade path is officially supported from Web Isolation versions 1.13, 1.12, 1.11 and 1.10.
For older versions please consult Symantec Technical Support:
https://www.broadcom.com/support/software/contact

After Upgrading from Version 1.12 and Earlier

Native Context Menu

Upgrading customers will default to the native context menu.

If you want to revert to the legacy custom Symantec context menu:

1. Go to each active Isolation Profile > Vector Rendering Settings > Context Menu.
2. Select the Symantec custom menu.
3. Push settings.

With the native context menu configured, there are two options to indicate to the end user that they are being isolated:

- User can press Ctrl + Q which will display the Advanced Options screen.
- You can configure isolated pages to display the Isolation Indication graphic mark:
    1. Go to Profiles->Isolation Profiles
    2. Under Miscellaneous, select Add a graphic mark to indicate an isolated website.

Adjustments to 'Isolation CPL Layer' for proxy chaining deployments

Solely for the Loopback scenario, in which ProxySG forwards traffic to the Symantec Threat Isolation Platform (STIP) and receives it back from the STIP before forwarding it to the Internet, insert the following line in the ProxySG 'Isolation CPL Layer', under Isolation_CondListIsolationServicesDestinationNoSSLInterception condition:

```
url.host.regex="fgl-fileserver[.]s3[.].*[.]amazonaws[.]com"
```

Before and After Upgrading from Version 1.11 and 1.10

For Votiro Disarmer customers running a Votiro API version lower than v3:

- Upgrading to Web Isolation version 1.14 upgrades Votiro API to version 3 without backward compatibility to earlier API versions. The following section describes the actions required to maintain Votiro Disarmer functionality post v1.14 upgrade:
- The following new Download Profile > Advanced Settings are introduced as part of Web Isolation v1.14:
  - votiro.api.baseUrl
  - votiro.api.key
- The following old Advanced Configuration Settings will be removed once upgrading to Web Isolation v1.14:
  - antivirus.votiro.api.hostname
  - antivirus.votiro.api.sendFileQuery
  - antivirus.votiro.api.getStatusQuery
  - antivirus.votiro.api.getRegularReportQuery
  - antivirus.votiro.api.downloadFileQuery
- The remaining Advanced Configuration Settings will be migrated when upgrading to the corresponding Download Profile Advanced Settings
- Actions required by **Votiro Disarmer Cloud** customers **Post Upgrade to Web Isolation v1.14**:
  - Obtain a Votiro API key from Votiro Customer Services
  - Set the Votiro API key in Web Isolation **Download Profile** > **Advanced Settings** > **votiro.api.key**
  - Push Settings
- Actions required by **Votiro Disarmer On-Premises** customers **Post Upgrade to Web Isolation v1.14**:
  - Upgrade Votiro On-Premises deployment to v3
  - Specify the On-Premises service URL in Web Isolation **Download Profile** > **Advanced Settings** > **votiro.api.key**
  - Set 0 (zero) as the Votiro API key in Web Isolation **Download Profile** > **Advanced Settings** > **votiro.api.key**
  - Push Settings

Before Upgrading from Version 1.10

IMPORTANT: When upgrading from version 1.10, Symantec Web Isolation Management version 1.14 cannot push settings to gateways running version 1.10.

- Before pushing settings, make sure all gateways have been upgraded to version 1.14.
- When some but not all gateways have been upgraded, push settings will succeed only for the 1.14 upgraded gateways, and fail for all others.

  The Gateways page will display an error indication in the Status column and a VALIDATION_ERROR in the Details column for each gateway for which push settings failed.

  To prevent these errors:

1. Upgrade the gateways that produce the error to version 1.14.
2. Push settings.

Known Limitations

End User Experience

	In video streaming mode, videos might partially hide nearby elements on the screen, for example while a video element is being scrolled (GRM only).
	Isolation is not supported for web sites with FTP schema.
	Native Context Menu 'Copy image address' function isn't supported. 'Search Google for image' function isn't supported. 'Save image as…' will save resource images with a pre-determined file name instead of the original file name.

Chrome End Users

	Google Chrome might display an error page when the proxy has no Internet connection.
	Google Chrome Translate Webpages feature is not supported.

Internet Explorer End Users

	Internet Explorer does not support copying of rich text.

Safari End Users

	Safari configuration pre-requisites End users using Safari need to configure the browser to always allow cookies, as follows: For older Safari versions, Open Safari > Preferences... > Privacy > Cookies and website data > Always allow For newer Safari versions, unselect Safari > Preferences... > Privacy > Website tracking > Prevent cross-site tracking

Gateway

	SSL trust: Elliptic Curve Digital Signature Algorithm (ECDSA) is not supported. Peer certificate (server certificate - not self-signed) trust applies in Isolate actions, but not in Inspect actions.

	When SSL termination is off, the following functionality is not supported: Vector Rendering Server Authentication
	Grid Rendering dynamically-updated list of URLs in Vector Rendering Isolation Profiles is not supported for environments with no Internet connectivity on the proxy.
	Post forwarding does not support chunked transfer encoding and is limited to a payload of 50K by default. The payload size limit is configurable.

File Downloads, File Uploads and File Viewer

	In the Download profile, archive options, the following archives are supported: zip, tar, gz, 7z, rar, xz, wim.
	Symantec document isolation does not support protected sheets in Excel files.
	On Document Isolation Viewer, using File -> Print is not supported. End users can print the document by clicking the print icon or using the keystroke of CTRL+P.
	Archive Sanitization (Archive Recompression for File Sanitizers): Supported filetypes: ○ Non-password protected archives: zip, tar, gz, 7z, xz, wim ○ Password protected archives: 7z and zip No support for archives containing files with multiple passwords

Management

	In Internet Explorer, Symantec Threat Isolation Management is not accessible when the proxy component resides on the Management server machine. Use Chrome or Firefox instead.
	SAML and RADIUS Management Users cannot be restricted to view Activity Logs of “Specific Organizations” and will default to “All Organizations”.

Related Documentation

For complete documentation of the Symantec Threat Isolation Platform, see the Symantec Threat Isolation Platform Guide for Administrators:

https://techdocs.broadcom.com/content/broadcom/techdocs/us/en/symantec-security-software/web-and-network-security/web-isolation/1-0/web-isolation-administration-guides.html