Trustwave®
Smart security on demand

Security Reporter 3.5.0 Release Notes

December 2016

Trustwave is pleased to announce the release of Security Reporter version 3.5.0. This software release requires a Trustwave Security Reporter appliance running software version 3.3.15, 3.3.20, 3.4.0, or 3.4.10, and will upgrade the Trustwave Security Reporter software version to 3.5.0.

Note: Upgrading a virtual SR to version 3.5 requires additional steps. For more information, see Trustwave Knowledgebase article Q20722.

SR 3.5 is a major update and Trustwave recommends you read this entire document carefully before proceeding to upgrade. For system requirements and update instructions, see the end of this document.

Supported Data Sources

This upgrade is compatible with Secure Web Gateway appliances running software version 11.6 or later, OR Web Filter appliances running software version 5.1.0 or later.

Note: Version 3.5.0 supports reporting on either SWG or Web Filter devices (one or more of either type), but you cannot report on both SWG and Web Filter data from the same SR.

You cannot upgrade to this version of SR if both SWG and WF devices are present in the Device Registry. Before upgrading from SR 3.3.15 you must ensure you have only one type of source device in the Device Registry.

Data Migration

Non-migrated historical reporting data (data that is still in version 3.2 format) is permanently deleted on upgrade to this version of SR, if it has not already been deleted in an earlier upgrade. Backups of data in the 3.2 format cannot be restored after upgrade. If you are upgrading from version 3.3.X and you want to save this data, you must complete migration before upgrading to this release.

- If any data would be lost during upgrade, the upgrade process requires the administrator to confirm the action.

Reports Deleted

All reports that were previously generated will be deleted on upgrade to this version of SR, including Scheduled and Executive Summary reports. You will be able to re-run the reports for data that has not expired. For Executive Summary reports, you can run a report covering the same time period, but the output format will differ.

Note: Before proceeding with the upgrade, be sure that all report users are notified. In particular if reports are delivered as links, each recipient should follow the links, and download any essential reports to another location.

Removed Functionality (applies to upgrades from 3.3.x):

- For SWG reporting, the Vulnerability Anti.dote channel and data has been removed from all reports. This feature is not present in currently supported releases of SWG.
- For Web Filter reporting, the Real-time Reports are no longer supported. All historical data related to real-time reports, including gauges, alerts, lockouts and trend charts, will be deleted permanently during the SR 3.5.0 upgrade.
- Language localization is no longer supported. The interface always displays in US English.

New Features

This release includes significant changes in a number of areas, along with minor enhancements and bug fixes.

For a summary of the changes made in this version, see below. Review all sections for versions newer than the version you are currently using. (If you are upgrading from 3.3.x review all sections; if upgrading from 3.4.0 review the 3.4.10 and 3.5.0 sections; if upgrading from 3.4.10 review the 3.5.0 section only.)

For more details on the minor changes, see the Resolved Issues section below. For full technical details, see the *Appliance Installation Guide* and the *Administrator Guide*. To download documentation, see the link at the end of these notes.

Changes new in 3.5.0

Operating System upgrade

SR now runs under the TrustOS operating system (version 2.5). TrustOS provides numerous security and functional enhancements.

The root password is restored to the default as a result of the operating system change. For any changes requiring root access, contact Trustwave TAC.

HTTPS update: SHA-2 Certificate Support

SR now supports SHA-2 certificates for HTTPS. The default certificate provided is a SHA-2 certificate.

Reports URL (Web Links) Change

The reports that were previously available from the main appliance user interface (port 8443) have been moved, to improve reliability with large outputs. All reports are available from a new web service on port 8843.

Enhancements to Specialized Reports

The Executive Summary, Blocked Request and Time Usage reports now use the framework provided by the Report Wizard.

Safer Shutdown and Restart; Longer timeouts for data summarization

The shutdown process has been revised to safely shut down the database system and wait longer for data summarization to complete. This change helps to prevent data corruption.

Enhanced Data Expiration

The data expiration processes are now more robust and considerably faster. The SR is less likely to suffer from disk space exhaustion.

Clickable Charts

Clicking a bar in the on-screen report output now performs the same action as a click on the associated data in the grid.

Software Updates and Changes

- MySQL has been updated to version 5.6.30.
- Tomcat has been updated to version 8.0.12.
- SR now uses Java 8 and Spring 4.
- BIRT has been updated to version 4.5.

Improved hardware and RAID status detection

The RAID status check and notification has been enhanced.

Enhanced Support Package

Additional items are included in the Support Package: Summarization status, disk I/O throughput RAID status, and service log files from runit wrapped services.

Additional client system support

SR supports Windows 10 as a client system.

SR supports macOS 10.12 (Sierra) and OS X 10.11 (El Capitan).

Changes new in 3.4.10

Optional secondary sort

SR provides a global option to sort report results on the Group By field if the primary sort is on another field. This option clarifies the returned results but requires additional processing time.

Enhanced filter selection

SR automatically adds “include all” to User Group and Report Filters if no other included items are selected. SR removes “include all” from these filters if a specific included item is selected.

Detail Report time headings

SR shows the selected times as well as the dates in the heading of detail reports.

Data storage and processing enhancements

Some data processing strategies have been optimized for better performance.

The "Detail result warning" for large record sets is no longer required and configuration for this option has been removed.

Vulnerability related updates

A number of modules have been updated to address recently reported vulnerabilities in open source software.

Changes new in 3.4.0

Support for Application Control

SR provides the ability to report on Application Control activity in the SWG. The new items include additional Summary Reports, and a new channel in the Report Wizard.

Support for Dynamic Categorization

SR provides the ability to report on Dynamic Categorization activity in the SWG. The new items include options on the General tab of the Report Wizard, counts in Summary Reports, and an available column in Detail Reports.

Support for IPv6

SR now supports IPv6 for system configuration, as well as for reporting data (where supported by the data source, currently SWG only). In fields that require entry of a network mask (either for IPv4 or IPv6), the mask is entered as a routing prefix length in CIDR notation.

Revised User Group page

The interface used to view and edit User Groups has been updated. Groups can now include IP ranges in CIDR notation. Existing groups are automatically updated to use the new format.

The User Groups listing now displays the names of Group Administrators assigned to each user group.

Revised Summary Reports menu

Summary Reports are now grouped, and selected from a menu instead of a thumbnail strip.

The date scopes "Week to Yesterday" and "Month to Yesterday" have been replaced by "Current Week" and "Current Month".

A new Summary Report, Top 20 Sites by Bandwidth, has been added.

The following existing reports have been moved and renamed:

- Top 20 User Group Comparison is now found under Top 20 User Groups by Page Count > Pie Chart
- Top 20 Categories Comparison is now found under Top 20 Categories by Page Count > Pie Chart

Bar charts are also available for these two reports.

Redesigned System Configuration Interface

The System Configuration interface has been updated to a standard menu driven interface. Some items have been moved to the Report Manager menus.

- A number of configuration items are now found on the Device Registry page.
- SR Activation is found on the Server Information page.
- A new menu item, Administration > Server Status, gives access to detailed information about system internals.

Safer Shutdown and Restart

The shutdown process has been revised to safely shut down the database system. This change helps to prevent data corruption.

Changes to Group Administrator permissions

Group Administrators can no longer edit or remove groups assigned to them.

Group Administrators can view the membership of groups assigned to them.

Access to view Summary Reports can be disabled for Group Administrators.

Known Issues

- Firefox users may experience minor display issues after upgrading to SR 3.5. For details and resolutions, see Trustwave Knowledgebase article Q20732.
- When the SR is upgraded from 3.3.x to 3.5, in some cases a patch completion message displays while some of the upgrade-related operations are still ongoing. If you click the link in the message before upgrade is complete, you are not able to access the SR web interface. If you encounter this issue, wait for some time before you try to access the SR web interface again. If you are not able to access the web interface after a significant amount of time, contact Trustwave TAC.

Resolved Issues

- For a list of Resolved Known Issues, browse to http://www.trustwave.com/software/8e6/ts/sr-rki.html. Click the SR 3.5.0 accordion section (and earlier version sections if upgrading from earlier versions) to view the resolved known issues for this software release.

System Requirements

This software release is available for the following hardware platforms:

Models 300, 500, 505, 700, 705, 730, 735

Browser requirements

The following minimum browser versions are tested and fully supported for access to the SR web interfaces:

- Internet Explorer 11
- Edge *(Note: Certificate management for Edge is performed in Internet Explorer.)*
- Firefox (current versions)

- Chrome (current versions)
- Safari 8

Earlier browser versions can generally be used to access the Report Manager. The System Configuration interface requires a HTML5 compliant browser.

Note: The latest versions of Safari (10) and Chrome (55) require user permission to run Flash for each site. For more information about how this change affects SR, see Trustwave Knowledgebase article Q20733.

Update Instructions

To update your supported Security Reporter appliance, see the Software Update section of the *Administrator Guide* or Software Update screen in the Console.

Notes:

- If the SR is currently processing a significant volume of logs, it could take up to ten hours for this software update to be installed.
- This update performs two system restarts to complete the installation. Do not turn the SR on or off manually during the installation process.
- All the reports stored on this SR will be deleted permanently during the upgrade. If you still want to download any report previously generated on this SR, do not proceed with the upgrade now. Instead, download the reports first and upgrade later.
- If this SR is configured to report on data from SWG policy servers, during the upgrade you will be asked to enter the SWG log feed password. If you do not have a record of this password, you must change the common SWG password on SR and enter the new password on all SWG servers.

Documentation

To download the full set of documentation that applies to this release, see https://www.trustwave.com/support/SR/

Legal Notice

While every precaution has been taken in the preparation of this document, Trustwave assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

While the authors have used their best efforts in preparing this document, they make no representation or warranties with respect to the accuracy or completeness of the contents of this document and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the author nor Trustwave shall be liable for any loss of profit or any commercial damages, including but not limited to direct, indirect, special, incidental, consequential, or other damages.

The most current version of this document may be obtained by contacting:

Trustwave Technical Support:
Phone: +1.800.363.1621
Email: tac@trustwave.com

Trademarks

Trustwave and the Trustwave logo are trademarks of Trustwave. Such trademarks shall not be used, copied, or disseminated in any manner without the prior written permission of Trustwave.

About Trustwave®

Trustwave helps businesses fight cybercrime, protect data and reduce security risk. With cloud and managed security services, integrated technologies and a team of security experts, ethical hackers and researchers, Trustwave enables businesses to transform the way they manage their information security and compliance programs. More than three million businesses are enrolled in the Trustwave TrustKeeper® cloud platform, through which Trustwave delivers automated, efficient and cost-effective threat, vulnerability and compliance management. Trustwave is headquartered in Chicago, with customers in 96 countries. For more information about Trustwave, visit https://www.trustwave.com.