Security Reporter 3.3.0 Release Notes

September 2013
Trustwave is pleased to announce the release of Security Reporter version 3.3.0. This software release requires a Trustwave Security Reporter appliance (or virtualized instance) running software version 3.2.0 and will upgrade the Trustwave Security Reporter software version to 3.3.0.

This upgrade is compatible with a Web Filter appliance running software version 5.1.0 or later, and/or a Secure Web Gateway appliance running software version 9.2 or later.

New Features

Security Reporter 3.3 includes significant changes in a number of areas, including administrator logons and permissions, and the Report Wizard. For a summary of changes, see 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.

Administrator Groups and Profiles

Administrator permissions are simplified. Only two permission levels exist: Global Administrator and Group Administrator. You can create additional Global Administrators. All Global Administrators can perform all administrative functions. Group Administrators have administrative power over all groups assigned to them.

Report Wizard

A single Report Wizard is now used for all Wizard functions. The Reports menu is simplified and reorganized to reflect this change.

The Report Wizard includes three tabs: General, Grouping & Visibility, and Filters.

- The General tab includes naming, date scope, export format, and include/exclude options.
- The Grouping & Visibility tab provides the ability to add levels of grouping, specify sorting criteria, limit the number of items at each level, and choose detail or summary reporting for the final level. This tab also allows you to select the data columns for reports, and change the order of columns.
- The Filters tab allows you to include or exclude specific logged items from a report (such as action, policy, site, user, or user group). You can also specify filter patterns that will be evaluated at the time a report is generated.

New SWG data available

- Reporting and filtering is now available for SWG X-Ray rules.
- Search strings are now extracted and displayed for SWG transactions.

Data Channels

Version 3.3 introduces the concept of data channels (generally related to report types): Category, Content Type, Rule, Spyware, Violation, Virus, and Vulnerability Anti.Dote. For each report type, you can filter based on items from the data channel (using the Report Wizard Filters tab).

New Report organization

In version 3.3 the path to access some reports has changed. The table below shows the locations in the console in version 3.2 and 3.3.

SR 3.2	SR 3.3
Reports > Drill Down Reports > Categories, IPs, Users, Sites, Category Groups, User Groups	Reports > Drill Down > Category (Use appropriate first level grouping in the Report Wizard – such as Category, IP, User, Site, Category Group, User Group)
Reports > Security Reports > • Blocked Viruses • Security Policy Violations • Traffic Analysis • Rule Transactions	Reports > Drill Down > • Virus • Violation • Content Type • Rule
Reports > Security Reports > Advanced Reports > • Vulnerability Anti.Dote • Spyware	Reports > Drill Down > • Vulnerability Anti.Dote • Spyware

Schedule and Saved Report screens

Records for Saved Reports now show the selected export format.

Saved Reports and Schedules now also show the name of the administrator that created the item. Global Administrators can now view items created by other administrators.

Data storage and processing enhancements

The database schema and data processing strategies have been optimized for better performance.

The Email Reports process now runs in the background and you can continue to work with the user interface while it is running.

MySQL has been updated to version 5.5.

Data migration

If you want to report on historical data using the version 3.3 reporting framework, you must migrate the data to a new format. Depending on the amount of data being migrated, migration could be a time-consuming process creating additional load on the SR.

Any data that is not migrated will continue to be available for reporting through the version 3.2 reporting framework also included in this release.

- When you upgrade, you have the option to start a backup and migration of existing data. You can choose the number of days of data to back up and migrate.
- You can change the backup and migration options later.
- The backup and migration runs in the background. You can monitor progress and change the selected options from the product web interface.
- For data that is not migrated, you can continue to use a limited set of features from the version 3.2 reporting framework, accessible from a link on the Report Manager console.

Evaluation Mode

All data imported during the evaluation period is now retained on the server and is unlocked for viewing once the SR is activated. Previously, data was only available for the latest, maximum three-week period, and was permanently removed once that period passed.

User Group deletions

Administrators can now delete all user groups assigned to them, except "system" groups.

Vulnerability mitigation

System components and behaviors have been updated to mitigate reported vulnerabilities.

Resolved Issues

- For a list of Resolved Known Issues, browse to http://www.trustwave.com/software/8e6/ts/sr-rki.html. Click the SR 3.3.0 accordion section 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

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.

Note: If the SR is currently processing a significant volume of logs, it could take several hours for this software update to be installed. Additionally, to take advantage of new features in version 3.3, you must migrate data to the new database format. Data migration could take days to complete (depending on the volume of data).

FAQ

Q: How long will it take for data backup and migration to finish?

A: It is not possible to give a general answer to this question because the volume and type of data differ between installations. Once the backup and migration has started, the web interface shows the progress of migration, including the rate of processing and estimated time remaining. You can pause the process or change the settings at any time.

Documentation

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

Legal Notice

The most current version of this document may be obtained from:

www.trustwave.com/support/

Trademarks

About Trustwave®

Trustwave is a leading provider of compliance, Web, application, network and data security solutions delivered through the cloud, managed security services, software and appliances. For organizations faced with today's challenging data security and compliance environment, Trustwave provides a unique approach with comprehensive solutions that include its TrustKeeper® portal and other proprietary security solutions. Trustwave has helped hundreds of thousands of organizations — ranging from Fortune 500 businesses and large financial institutions to small and medium-sized retailers — manage compliance and secure their network infrastructures, data communications and critical information assets. Trustwave is headquartered in Chicago with offices worldwide. For more information, visit https://www.trustwave.com.