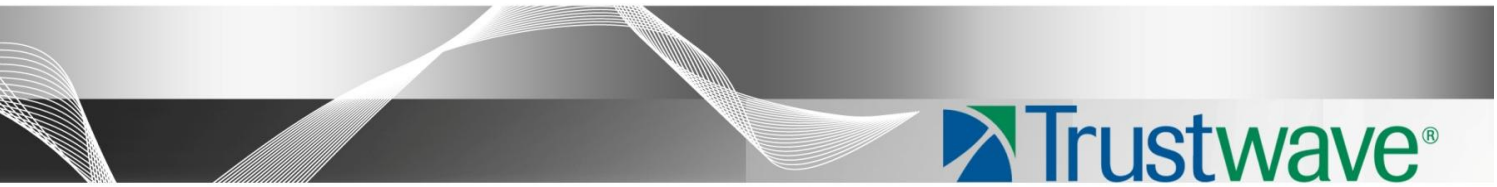

Secure Web Gateway

Version 11.0

Release Notes

Legal Notice

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

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

Trademarks

Table of Contents

Legal Notice 2
Trademarks 2
Table of Contents 3
Secure Web Gateway 11.0 (GA) Release Notes 4
New Features 4
ICAP (Internet Content Adaptation Protocol) Client Support 4
Manageability and Scalability Enhancement 4
Enhanced Trojan Detection 5
Enhanced Detection of Malicious SWF files 5
New Hybrid Solution Features 5
General Enhancements and Bug Fixes 5
On-Box Reporter Enhancements 6
Improved User Management 7
Cloud Configuration Enhancements 8
Enhanced Logging Capabilities 8
Dashboard Enhancements 9
Streamlined Policy Management 9
GUI Enhancements 10
Hardware Requirements 10
How to Install This Release 11
Documentation 11

Secure Web Gateway 11.0 (GA) Release Notes

Trustwave is pleased to announce that Secure Web Gateway version 11.0 is available on a General Availability basis. Review the Release Notes below for further information.

New Features

ICAP (Internet Content Adaptation Protocol) Client Support

With version 11.0, Trustwave introduces the ICAP RESPMOD (Response Modification), which enables SWG to communicate with all types of ICAP servers or client devices. ICAP, the Internet Content Adaption Protocol, is a lightweight protocol for executing a "remote procedure call" on HTTP messages. This enhancement completes the support for ICAP REQMOD, which was introduced in version 10.2. This new functionality enables integration with other Trustwave products, such as Trustwave DLP Protect.

Manageability and Scalability Enhancement

In this version, Trustwave has invested in improving the usability of the system, based on intensive field research. The list below includes the highlights of these features:

- **New Upgrade and Downgrade Mechanism:** The administrator can now upgrade devices from the system UI, without the need for physical access to the devices. (Trustwave Internal #38061)
- **New Home Page:** The new Home Page serves as the entry point to the application Management Console UI, and includes links to frequently used tasks, commonly used reports and charts, information on pending updates and system log information.
- **Semantic Search:** The administrator can now search for any object or menu item in the system using one search box, accessible on every page of the application.
- **New Update Mechanism:** For each update type, the administrator can now easily define the checking interval for updates and the behavior once the pending update is pulled. (Trustwave Internal #38952)
- **New Log View:** The Log View, one of the most common day-to-day tasks, is improved by enabling extended search options and enhanced profile management.
- **Streamlined Security Policies:** The out-of-the-box set of policies is now streamlined, and the terminology used is standardized and comprehensive. The simplified and advanced options are removed, and the system comes with one default security policy that can be adjusted to the customer's needs.
- **Improved Scalability:** The system can now support highly distributed environments without impacting system performance.

Enhanced Trojan Detection

As utilization of the HTTP protocol by cybercriminals to implement botnets rapidly grows, SWG can now intercept malicious communication as part of its built-in outbound scanning capabilities. With version 11.0, Trustwave introduces a solution based on identifying communication to C&C servers, using an up-to-date list that is independent from the source of infection. Version 11.0 also introduces new reports on the derived transactions to enable tracking and cleaning of infected machines. (Trustwave Internal #39388, 39387)

Enhanced Detection of Malicious SWF files

SWF files have become a popular exploit and attack vector on the web. SWG 11.0 introduces improved detection capabilities in the Binary VAD engine for malicious Adobe Flash files.

New Hybrid Solution Features

- Support for Apple OS X Mountain Lion (10.8)
- **On-premise PAC file option:** MSC configuration can be optimized by using the customer's standard PAC file when on-premise and the SWG-maintained PAC file when off-premise.
- **Automated upgrades for local Cloud Scanners:** Local Cloud Scanners (not Amazon EC2) can now be upgraded in the same way as other SWG Scanners, saving administrator time and effort while simplifying the upgrade process.
- **User certificate management actions can be performed concurrently on multiple users:** Administrator time is saved by allowing certificate actions (e.g. issue, revoke etc.) to be applied concurrently to multiple users based on selection criteria, including group names.
- **Client code auto-update controlled by group membership:** Updating MSC code by user group enables the phased roll-out of new MSC versions.
- **Client connectivity failure behavior control**: When the MSC cannot connect to any Cloud Scanners, connectivity can be set to disable, direct or adjustable hotel mode, according to company policy (set by SWG Policy Server).
- **User Certificate enforcement options:** Provides control over the level of access allowed if a user certificate is not provided when the client is installed. This can help simplify client set-up in situations where user identification is not needed.

General Enhancements and Bug Fixes

- Switch CFM to opt-out model (Trustwave Internal #38423)
- Rebranding of UI to Trustwave (Trustwave Internal #38943)
- SWG now blocks sites that use certificates that were signed by keys with length less than 1024 bit (Trustwave Internal #39004)
- Fixed the issue of during a long commit, Notifier will not send status requests to scanners (Trustwave Internal #37699)
- SNMP | SNMPv2 community name is now rebranded to Trustwave (Trustwave Internal #35377)

- Fixed SWG returning 502 error when a POST request is answered by a '100 Continue' (Trustwave Internal #39402)
- Fixed wasp.log getting filled with messages about module.xml (Trustwave Internal #38963)
- Removed the option 'used in' in the Digital Certificate Store (Trustwave Internal #38695)
- Added CA validation for HTTPs, Cloud PKI mode and Cloud Internal mode (Trustwave Internal #38648, 38649, 38650)
- Valid SMTP characters are now supported (Trustwave Internal #38241)
- Update downloads now supports resume downloads in order to be more resilient (Trustwave Internal #37871)
- Changes done by an admin are now committed after admin name change (Trustwave Internal #37478)
- In FTP, "Block Unscannable" is now propagated to FTP client side (Trustwave Internal #35751)
- In Syslog, the message "Commit Changes successful" in Audit Log is now received in "Syslog Daemon" (Trustwave Internal #34618)
- Fixed the failure of recovery from failed xdelta based security updates (Trustwave Internal #38589)
- MP4 files are now recognized correctly (Trustwave Internal #38717)
- File type of PDFs is now correctly detected on upload (Trustwave Internal #38635)
- Fixed DB backup Restore page not showing all files from FTP server (Trustwave Internal #36116)
- Upstream proxy protocol fields are not mandatory, and the user should be able to add proxy for just one protocol (Trustwave Internal #38486)
- Added support of sending data to Syslog in TCP (Trustwave Internal #39275)
- Upgraded Kaspersky SDK to 8.1.3.141 version (Trustwave Internal #39400)

On-Box Reporter Enhancements

- Reports' description adjusted (Trustwave Internal #39623)
- Fixed failure in running 'Unknown Threats - Behavior Based' report and adjusted sorting and sub-totals (Trustwave Internal #39557, 33810)
- Changed name to Infected Machines report (Trustwave Internal #39497)
- Security Policy Violations report and chart is now sorted by count URLs (Trustwave Internal #39471)
- Trustwave Web Filter reports does not appear now if the license is for other URL filtering engines (Trustwave Internal #39320)
- Removed the "Repaired Pages with Suspicious Code" report (Trustwave Internal #39211)
- Added the Malware Entrapment Report (Trustwave Internal #39120)
- Fixed the ability to bypass permissions when running reports (Trustwave Internal #38953)

- Added the category name to the 'Web site categories violating policy' report (Trustwave Internal #38946)
- Added the ability to change a report's instance for "run in the background" option (Trustwave Internal #38492)
- Fixed "Top Domain Names by Security Rule" report numbering (Trustwave Internal #36465)
- Fixed problems with specific fonts in report names (Trustwave Internal #36226, 36225)
- Fixed the behavior where "Authenticated users=All" filter does not apply (Trustwave Internal #36425)
- Fixed failure in displaying HTML reports on VM once there is a large amount of data to present (Trustwave Internal #36051)
- Fixed viewing of failed reports (Trustwave Internal #35962, 35963)
- Added 'Traffic Analysis - Raw Data' report to all customers, even when URL categorization is not installed (Trustwave Internal #38499)
- Report scheduled to 00:00 now shows results from the last day (Trustwave Internal #38484)
- "Adware Sites Accessed by User" report now presents data, which is grouped by user (Trustwave Internal #36462)
- A failed connection test in Report Backup will generate an invalid vsalert message user (Trustwave Internal #39299)

Improved User Management

- Fixed User Lists not being applied as an exception when the group included in the User List has 2 or more IP ranges (Trustwave Internal #39350)
- Fixed "User Groups/Users using this policy" pane not showing LDAP groups (Trustwave Internal #38845)
- Fixed password change enforced for a new user at first login even when option is not selected (Trustwave Internal #38551)
- Importing more than 1000 users/groups for SUN directories is now supported (Trustwave Internal #37041)
- Fixed truncating user credentials when using a long username (Trustwave Internal #39771)
- Fixed the error received while saving a custom LDAP after importing LDAP Users (Trustwave Internal #38590)
- Fixed failure when adding certain regular expression as URL condition (Trustwave Internal #38580)
- Fixed failure when removing passive device from devices tree saying "Failed to save data: Transaction not successfully started." (Trustwave Internal #38509)
- Fixed restoring from rollback ending with the system being unusable (Trustwave Internal #38507)

Cloud Configuration Enhancements

- In Blocked/Revoked cloud user (internal mode), block page now includes transaction ID (Trustwave Internal #38539)
- System GUI now indicates when installing a server certificate instead of a CA (cloud internal mode) (Trustwave Internal #38537)
- Added warning on a cloud scanner running in non-private configuration (Trustwave Internal #38413)
- Filter is now saved in Cloud users' screen (Trustwave Internal #38408)
- Enhanced the process for issuing certificate to all unassigned cloud users (Trustwave Internal #38398)
- Cloud scanner selection sequence can be adjusted (Trustwave Internal #39112).
- Client code auto-update can be enabled/disabled globally (Trustwave Internal #39264).
- Local Cloud Scanners can now be managed from in internal IP address (Trustwave Internal #38421).

Enhanced Logging Capabilities

- Fixed the behavior of alerts generated by SNMP in system logs showing information from scanner as originating from PS (Trustwave Internal #38879)
- Fixed the issue of many logs missing in system logs after upgrade (Trustwave Internal #38852)
- Added the export option to csv or xml on a specific log entry (Trustwave Internal #38827)
- Added ad-hoc search capabilities in the log viewer (Trustwave Internal #38826)
- Changed the main logging screen (Trustwave Internal #38825)
- Moved logs' view management to a tree in the left pane (Trustwave Internal #38824)
- Fixed the display of the paging (Trustwave Internal #38691)
- Added the option to copy/paste text from system log (Trustwave Internal #38657)
- Fixed the issue of logs not being collected from all relevant partitions (Trustwave Internal #38546)
- User name is now logged when authentication fails (Trustwave Internal #34815)
- "ICAP Service Name" and "ICAP Block Reason" added to web log details (Trustwave Internal #38776)
- Added an indication in the log views that there is a filter (Trustwave Internal #39279)
- SWG now supports "I18N - international characters" on Block Reason in Web logs (Trustwave Internal #38565)
- Removed the "Admin HTML Repaired Transactions" view (Trustwave Internal #39119)
- Extended the retention period to 3 figures (Trustwave Internal #38504)
- Time format in audit log is now consistent with web and system logs (Trustwave Internal #38493)
- Fixed Audit Log presenting "0" in module field instead the correct value (Trustwave Internal #38491)

- Fixed Error message received while dragging a column title to "Log ID" (Trustwave Internal #38488)
- Fixing the retention management requiring a transaction on the new days to trigger deletion process (Trustwave Internal #38315)
- When system is configured to send audit to syslog log, an extra "commit changes completed" message is no longer added to system log (Trustwave Internal #38313)
- Log details view now looks the same as the log details of the log entry wizard (Trustwave Internal #38245)
- Changed the behavior of the Web Logs time filtering (Trustwave Internal #37086)
- Fixed when updating User Email and committing, the Audit Log displaying: "Nothing to commit." (Trustwave Internal #36470)
- Audit logs are now sent when there are non-ASCII characters (Trustwave Internal #35005)
- In HTTPs running "Apply Default Values", doesn't send Certificate to scanner (Trustwave Internal #33652)
- Web log transactions are now sorted by absolute time (not scanner time) (Trustwave Internal #33131)
- Fixed performance issue in system/web log viewer with many scanners (Trustwave Internal #39665)

Dashboard Enhancements

- The device group is now shown on the Devices list (Trustwave Internal #39030)
- There is an option to delete messages from the Messages pane (Trustwave Internal #38665)

Streamlined Policy Management

- Condition Settings is changed to Condition Elements (Trustwave Internal #38685)
- Removed the "Block Outgoing Microsoft Office Documents" x-ray rule as it is obsolete (Trustwave Internal #35858)
- Fixed the issue of logging policy not logging bypassed transactions (Trustwave Internal #39477)
- In Identification policies the user can now view a condition of a rule whose name contains a colon (Trustwave Internal #35866)
- In HTTPS Policies when exporting to XML, fixed the exported fields (Trustwave Internal #35860, 35859)
- When exporting policies to HTML, fixed the wording to match the GUI (Trustwave Internal #35856)
- When exporting policies to HTML and XML Entrapment Rules are now exported in a clear way (Trustwave Internal #35854)
- When exporting policies to HTML and XML conditions are now sorted (Trustwave Internal #35853)

- Changed Security Policies concept. Basic, Medium and Strict built in policies are replaced with one "Trustwave Default Security Policy". The simplified and advanced options are omitted (Trustwave Internal 38319, 39576)

GUI Enhancements

- Added tootltip to icons in policies tree view (Trustwave Internal #39074)
- Changed Security Settings under Alerts to Security Alerts Settings (Trustwave Internal #38686)
- Fixed menu appearing as grayed out after cancelling a 'Change Password' operation (Trustwave Internal #38555)
- Permissions' grid view is now working on chrome (Trustwave Internal #38396)
- Virtual IP field values are now being validated (Trustwave Internal #38389)
- Changed terminology and UI in ICAP Client (Trustwave Internal #38249)
- Added options to delete Active Content List from Blocked / Allowed (Trustwave Internal #38308)
- Renamed the Rollback menu options (Trustwave Internal #39522)

Hardware Requirements

The following SWG appliances are supported:

- NG-5000-S1 (IBM Model 3350) *
- SWG 3000/NG5000-S2 (IBM Model 3250 M3)
- SWG 3000/NG5000-S2 (IBM Model 3550 M4)
- NG-6000-S (IBM Model X3650) *
- SWG 5000/NG-6000-S1 (IBM Model X3550 M2)
- SWG 5000 (IBM Model X3550 M3) *
- SWG 5000 (IBM Model X3550 M4)
- NG-8100-S (IBM Model HS21 8853)
- SWG 7100/NG8100-S1 (IBM Model HS22 7870)
- SWG 7100/NG8100-S1 (IBM Model HS23 7875)
- NG-8080-S (IBM Model HS21 8853)
- SWG 7080/NG8080-S1 (IBM Model HS22 7870)
- SWG 7080/NG8080-S1 (IBM Model HS23 7875)

***NOTE:** SWG 11.0 requires a minimum of 4GB RAM. The marked appliances are shipped originally with 2GB RAM. In order to purchase additional memory, contact your Trustwave Channel Partner/Account manager.

For more information, review the SWG Hardware Support Matrix.

How to Install This Release

In order to install this release, refer to the Downloads / Documentation section of the Trustwave website for the following documents:

- SWG Installation Utility - Technical Brief
- USB Key Creator - Technical Brief

Notes:

1. See the instructions below for installation on a High Availability Policy Server environment.
2. SWG Installation Utility version 1.6.0-13 is required.

High Availability Policy Server Installation:

1. Deactivate High Availability on the Passive Policy Server from the Active by logging in to the Management Console on the Active Policy Server and clicking **Administration** -> **System Settings** -> Expand the node of the **Active Policy Server** and click **High Availability** -> click **Edit** -> uncheck **Enable High Availability Policy Server** -> click **Save**.
2. Install SWG 11.0 on the Active Policy Server (using the instructions above).
3. Install SWG 11.0 (clean installation) on the Passive Policy Server.
4. Activate the Passive Policy Server by logging in to the Management Console on the Active Policy Server and clicking **Administration** -> **System Settings** -> Expand the node of the Active Policy Server and click on **High Availability** -> click on **Edit ->** check **Enable High Availability Policy Server** -> click **Save**.

Documentation

The following documentation is available for version 11.0:

- Management Console Reference Guide
- Setup Guide

The following documentation is available for the Hybrid deployment:

- Hybrid Deployment Guide
- Amazon EC2 Platform Setup Guide
- Mobile Security Client Administration Guide

About Trustwave®

Trustwave is a leading provider of information security and compliance management solutions to large and small businesses thought the world. Trustwave analyzes, protects and validates an organization's data management infrastructure from the network to the application layer – to ensure the protection of information and compliance with industry standards and regulations such as the PCI DSS and ISO 27002, among others. Financial institutions, large and small retailers, global electric exchanges, educational institutions, business service firms and government agencies rely on Trustwave. The company's solutions include on-demand compliance management, managed security services, digital certificates and 24x7 multilingual support. Trustwave is headquartered in Chicago with offices throughout North America, South America, Europe, the Middle East, Africa, Asia, and Australia.

