Secure Web Gateway 11.5 Release Notes

Trustwave is pleased to announce the release of Secure Web Gateway version 11.5.

Review the Release Notes below for further information.

Contents

New Features

Social Media Control (Trustwave Internal #40809)

Business use of Web 2.0 applications is growing exponentially, and presents a number of security, compliance, and productivity challenges. In this version, Trustwave assists enterprises to mitigate these issues by providing the ability to granularly control the use of common social media applications by users.

The social media applications that are supported are Facebook, LinkedIn, Google+, YouTube and Twitter.

The administrator can define which specific activities to block for which groups of users, or even for which individual users. The feature is integrated into the existing system infrastructure.

A built-in set of profiles is defined with this new feature. The profile set can be easily adjusted to the customer's own definition. For more information, see the *SWG Application Control User Brief*.

Improved Audit Log Module (Trustwave Internal #40826)

In version 11.5, an enriched Audit Log is added. All changes made to the system configuration are logged with a higher level of detail. The data is presented in a way that can be searched and sorted.

The information includes: who performed the operation, when, in which system and on which specific objects.

The same information is also introduced in the Commit Changes screen, where the list of operations that are about to be committed can be viewed in a separate tab.

Improved Performance

In this release, Trustwave has also invested in the infrastructure of the system. One major enhancement is the support for 64 bit infrastructure. These changes result in significant performance improvements and overall system efficiency in the SWG5000 M4 and HS23 blade models. This essentially means that each of the SWG devices is able to process more data in a given period.

New performance details will be published once the release is available.

Improved Security

SWG provides improved scanning of suspicious Adobe Acrobat Reader files and blocks malicious redirections from Traffic Direction Systems (TDS) servers.

Enhanced Authentication Options

With version 11.5, SWG now supports the secured Kerberos authentication mechanism, defined as an integral part of the system under User authentication directories. The administrator can easily utilize the benefits of Kerberos, where the protocol relies on secret keys that are transmitted in an encryption that cannot be intercepted. If the security of a network is compromised, it is still not possible for trespassers to interpret the content of network communications. User authentication and target services remain secure.

Dynamic Categorization

Version 11.5 introduces a new engine, the TextCensor, which dynamically classifies Web pages and files based on their content. The engine is used enhance the DLP capabilities of the system, and as a complementary solution for the URL filtering engine.

Usability and Scalability Enhancements

As part of its ongoing investment in system ease-of-use, Trustwave has added enhancements to the system's user interface and basic functionality. One of the major enhancements in this area is the linkage between objects and their main definition screen. For example, condition values in the policy configuration area are now linked to their respective condition elements screen.

SWG 11.5 can also now scale to support large and globally dispersed enterprises, by supporting up to 150 scanners, grouped in multiple groups and distributed around the world.

Enhanced URL Filtering

SWG version 11.0 is the last version that supports IBM and Websense URL filtering. Trustwave SWG is no longer reliant on third party vendors for URL filtering engines and SWG 11.5 is offered with the Trustwave proprietary URL Filtering engine.

Changes to MIB

The MIB (Management Information Base) definition file has changed. A MIB definition file, called TRUSTWAVESWG-MIB.txt, is available from the Trustwave website. This file should be imported into your SNMP monitoring software.

General Enhancements and Bug Fixes

- IPv6 configuration is now disabled by default (Trustwave Internal #41194)
- Old social media control rules are now removed from Default Security Policy (Trustwave Internal #41187)
- In URL Lists, exported and imported XML and CSV data now includes the description along with the URL entries (Trustwave Internal #41077)
- In URL Lists, the search option on URL entries now also searches in the description field (Trustwave Internal #41076)
- Restricted administrator can now add URLs to URL lists (Trustwave Internal #41035)
- The password reset script now also sets the UI password (Trustwave Internal #40971)
- Under Administration > System Settings > SWG Devices, in HTTPS Advanced tab settings, the default is now set to Allow Certificate Wildcards (Trustwave Internal #40915)
- The Updates Downloader URL is now set to the new Trustwave URL: swgupdate.trustwave.com(Trustwave Internal #40859)
- Fixed issue with running coached transactions on specific HTTPS sites (Trustwave Internal #40828)
- Fixed the show_config error of "List Index is out of range" (Trustwave Internal #40765)
- Fixed the break of High Availability after rebooting Policy Server (Trustwave Internal #40740)
- Fixed access to PDF files failing with "Invalid format" (Trustwave Internal #40707)
- Fixed Downloader to receive new configuration before it is restarted (Trustwave Internal #40667)
- Added correlation between SWG and BlueCoat events by using the x-virus-id header (Trustwave Internal #40604, 39856)
- Enhanced the scalability of the system by adding support for 150 scanners with one Policy Server (Trustwave Internal #40596)
- Added the limited shell command to show hardware specs (Trustwave Internal #40500)

- Fixed the behavior of broken gzip handling, which resulted in "Invalid format" (Trustwave Internal #40487)
- Proxy configuration set through the Configuration Management screen is now used for license validation (Trustwave Internal #40412)
- Regular administrator now has permissions on Web Log view and can open it (Trustwave Internal #40389)
- Fixed the issue of renewal of Kaspersky license key scanners stopping synchronizing (Trustwave Internal #40262)
- Added indication in System Log of failed connection between devices in the same group (Trustwave Internal #40198)
- Device IP is now logged on Audit Log when login fails (Trustwave Internal #40151)
- Added the option in the UI to control server side active/passive mode in FTP Native (Trustwave Internal #39980)
- Fixed ICAP HTTPS transaction appearing as ICAP/HTTP in Web Logs (Trustwave Internal #39936)
- Fixed the message "No connection to the Policy Server for more than 5 minutes" appearing after successful commit (Trustwave Internal #39926)
- Fixed Update configuration failing due to SSL Process (Trustwave Internal #39917)
- Fixed "Bad Request" appearing when browsing to https://secure.eicar.org/ in transparent mode (Trustwave Internal #39915)
- Fixed the alerts generated by SNMP in System Logs showing information from scanner as originating from Policy Server (Trustwave Internal #39852)
- Fixed Web Log entry missing when wrong domain provided for Authentication (Trustwave Internal #39688)
- Added rule names to be on the searchable objects list in the general Search box (Trustwave Internal #39314)
- Added "Check connectivity" option to the device options from the UI (Trustwave Internal #39176)
- Added logging of HTTP errors (for non-browser initiated requests) (Trustwave Internal #31002)
- Fixed ICAP health check failure when listening IP is defined (Trustwave Internal #40469)
- Added limitation of 1024-bit Maximum Certificate Key Length (Trustwave Internal #40090)
- Squid now supports specifying HTTP/1.1 connections to Web servers (Trustwave Internal #38547)
- Manager configuration now supports enabling/disabling a process depending on machine role (Trustwave Internal #38065)

On-Box Reporter Enhancements

- Updated "Potentially Malicious Websites" to include the transactions that are blocked by TextCensor (Trustwave Internal #41384)
- Adjusted the "Unknown Threats - Behavior Based" report which uses a rule that was removed (Trustwave Internal #40923)
- Fixed aggregation missing in reports (Trustwave Internal #40666, #40665)
- Fixed bandwidth data displayed as Bytes instead of KB in some reports (Trustwave Internal #40041)
- Fixed reports for the last N days not being created when using Middle East time zone (Trustwave Internal #39357)

Improved User Management

- Added warning of users becoming unassigned when importing users before importing groups (Trustwave Internal #41352)
- Fixed SWG reporting duplicate user entries on LDAP import (Trustwave Internal #40963)
- Fixed being able to create more than one LDAP directory with the same name (Trustwave Internal #40745)
- Fixed not being able to add groups to LDAP directories (Trustwave Internal #40460)
- Fixed users not assigned to "Domain Users" group in Cloud Certificate Management GUI (Trustwave Internal #40121)
- Fixed issues dealing with large number of groups and users (Trustwave Internal #39942, #39940)
- Fixed Base DN returning error of missing netBIOS name (Trustwave Internal #39373)
- Fixed the conflict with LDAP directories using similar names with space character in it (Trustwave Internal #39012)
- Destination IP is now logged if caching is enabled (Trustwave Internal #33950)
- Added support for Kerberos for end-user authentication/identification (Trustwave Internal #33351)

Cloud Configuration Enhancements

- Enhanced the design of management pages by splitting into several screens (Trustwave Internal #41029)
- In PKI mode the administrator can use Self-Signed CA (Trustwave Internal #40856)
- Added the Event Logger option (Trustwave Internal #40851)
- Enhanced Simple Client Mode by supporting automatic distribution of certificates (Trustwave Internal #40836)

- In the Bypass tab the administrator can now select multiple "Trusted URLs" (Trustwave Internal #40797).
- In PKI mode the generic certificate import from CSR now verifies for correct values (Trustwave Internal #40113).
- Fixed the error message received when trying to create a Generic certificate in PKI Mode (Trustwave Internal #39994)
- Fixed in PKI mode changed the defaults to unknown user (Trustwave Internal #40072)
- Fixed modifying generic CA not replacing original timestamp (Trustwave Internal #40061)
- Fixed not being able to delete on/off-premise indicator host name (Trustwave Internal #39965)
- Fixed the error message received when trying to send a provisioning email (Trustwave Internal #40028)

Enhanced Logging Capabilities

- Enhanced Audit Log Filter fields (Trustwave Internal #41290, 41291, 41289)
- Audit Log now shows icons instead of text in Committed and Action columns (Trustwave Internal #41141)
- Fixed Web Log auto refresh (Trustwave Internal #40748)
- Admin list is now sorted in Audit Log (Trustwave Internal #41280)

Dashboard Enhancements

- Fixed the issues when opening the Dashboard Graphs not being generated (Trustwave Internal #40418)

GUI Enhancements

- Added link functionality to ease navigation (Trustwave Internal #41114)
- In Import/Export screen fixed item names (Trustwave Internal #40821, 40821)
- Added in the UI the status of a service when it is enabled and its status is inactive (Trustwave Internal #40623)
- Fixed reordering columns not working correctly in Web Logs (Trustwave Internal #40550)
- Changed icons in the Help section (Trustwave Internal #40027)
- Changed the default password to the Management Console (Trustwave Internal #40008)

- Fixed **Select/Deselect all** option missing in the URL Filtering condition (Trustwave Internal #39975)
- Changed the title Trustwave Devices to SWG Devices (Trustwave Internal #39544)

Limitations and Known Issues

- SWG support for NTLM is limited - some features in newer versions of NTLM are not supported. (Trustwave Internal #41039)

  When using SWG Authentication mode "Negotiate" with NTLM (Negotiate NTLM, not the regular raw NTLM), this causes the client to halt the authentication process before completion if the LMCompatibilityLevel parameter in the client is set to 3 (the default value for Win7, Win2008SRV, and newer Windows versions).

  Workaround: Do not use Authentication mode "Negotiate" if planning to use NTLM. The authentication process will work in the same way as in version 11.0. If Negotiate mode is required and there are some appliances that do not support Kerberos, they will authenticate using NTLM, so the LMCompatibilityLevel parameter must be set (manually or by group policy) to LM=2 on these appliances.
- Uncommitted changes to setup settings for a device made by the administrator of one group are automatically committed when the administrator of another group performs a Commit Change action. (Trustwave Internal #39704)
- Coach actions cannot be used with URL Categorization - Coach actions work with URL Categorization on requests only, and dynamic categorization is applied to responses. (Trustwave Internal #41429)

  Workarounds:

  1. Do not use Coach actions for transactions blocked as a result of dynamic categorization.
  2. Fetch the content of the page out-of-line on the request, apply dynamic categorization on the fetched content, and then proceed as normal.

Hardware Requirements

The following SWG appliances are supported:

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

- SWG 7080/NG8080-S1 (IBM Model HS23 7875)

Note: SWG 11.5 requires a minimum of 4GB RAM. The appliances marked with * are shipped originally with 2GB RAM. To purchase additional memory, contact your Trustwave Channel Partner/Account Manager.
For more information, see the Secure Web Gateway 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:

SWG Installation Utility version 1.7.0.05 is required.

Legal Notice

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

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.