Secure Web Gateway 11.6 Release Notes

Trustwave is pleased to announce the release of Secure Web Gateway version 11.6.

November 2014

For information on upgrading, see the Trustwave SWG 11.6 Upgrade Release Notes.

Contents

New Features

IPv6 Support

In addition to IPv4, SWG now supports the IPv6 communications protocol.

- Device groups can be configured either for IPv4 or for IPv6. The protocol for the default Device Group and for user-defined Device Groups can be selected in **Administration | System Settings | SWG Devices**.
- When using transparent and Kerberos/NTLM authentication, SWG 11.6 requires two different hosts, one for IPv4 and another for IPv6. Each should be resolvable only to ONE IPv4 and ONE IPv6 address respectively. The IPv4 and IPv6 hostnames to which browsers in the system should be redirected must be specified in **Administration | System Settings | SWG Devices | Device | Scanning Server | Authentication | Advanced** tab.

TrustOS/TrustedSentry Integration

SWG now runs on the TrustOS operating system and TrustedSentry appliances.

- **TrustOS** provides a common software platform designed specifically for Trustwave appliances that unifies our on-premise security technologies and enables secure communication with the Trustwave cloud.
- **TrustedSentry** standardized hardware appliances are purpose-built for Trustwave and support better performance, capacity and redundancy.

This unified platform provides greater efficiency by allowing for easy scaling and rapid integration across Trustwave products, as well as third-party solutions.

SWG 11.6 continues to support the existing SWG appliances. For a list of supported models in 11.6, see Supported Appliances.

Transport Layer Security (TLS)

In addition to TLS version 1, SWG now supports options to enable TLS versions 1.1 and 1.2 in the HTTPS Service configuration.

Web Cache Communication Protocol (WCCP)

SWG 11.6 now supports WCCP version 2.01, which allows the use of IPv6 in WCCP-enabled routers and switches. Both the IPv4 and new IPv6 tabs enable the configuration of WCCP services with configurable service IDs and relative weighting.

Policy Test

The new Policy Test feature enables you to test a security policy for specific users and sites. You can also test specific URLs and files against the default security policy.

DLP Script Test

The new DLP Script Test feature enables you to check Data Loss Prevention scripts against the contents of a file or against specific text.

Tab Customization

A new Startup Tabs option tab in Administrative Settings enables you to define the tabs that open when SWG is launched after a refresh or logout.

Exporting Logs

You can now export Web log, System log, and Audit log results to a file. All the entries from the log database that match search criteria are downloaded in csv format, compressed to a .gz archive.

Scanner IP in Block Page

You can now customize the block page to include the IP of the scanner that blocked the transaction.

Port Scanning Protection

The new Port Scanning protection feature identifies multiple unsuccessful attempts to connect to a device and will block the originating IP for 20 minutes. It is enabled by default.

Load Policy Server Certificate

The option to replace the current default self-signed Policy Server certificate. CSR or Load certificate has been added.

Other Enhancements

- This release includes enhancements to the Trustwave Default Security Policy. Following extensive research, the changes are designed to improve the Trustwave SWG experience out-of-the-box, without interfering with our high security standards or users' daily tasks. All core security rules are preserved to continue the expected level of safety for users relying on Trustwave SWG. Our new policy doesn't reduce expected functionality and any rule from the legacy default policy can be added manually.
- DLP (Data Loss Prevention) built-in scripts have been extended to cover PCI Data Security Standards (PCI-DSS), protected health information (PHI), and personally identifiable information (PII).

Limitations and Known Issues

- Native FTP does not support IPv6
- Policy Server HA does not support IPv6
- WCCP with Generic Routing Encapsulation (GRE) is not supported with IPv6
- SWG support for NTLM is limited - some features in newer versions of NTLM are not supported.

  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.
- Coach actions cannot be used with URL Categorization - Coach actions work with URL Categorization on requests only, and dynamic categorization is applied to responses.

  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.

Resolved Issues

- Clicking Cancel when adding an item in the Wizard made the wizard unresponsive until refreshed
- Screen display was not satisfactory and an error message opened when searching "Limited Interactivity" in the Search field
- Breadcrumb navigation did not work properly in specific situations
- DLP condition syntax strings with \? or * changed after saving twice
- Transaction details were not presented when clicking on the Transaction ID after viewing user details
- DLP expressions in User details were not visible in the Wizard
- DLP expression validation was skipped when creating a new DLP script in Internet Explorer
- Commit failed after adding an IPv6 scanner
- The URL Category column was not filled in the Weblog for category "Other"
- ACU was not listed in System Information
- Group import failed when an LDAP group identifier was empty
- Could not set permissions for a Web Log Admin group of super administrators to more than None
- Independent users could not be moved into a group
- Could not define an LDAP Directory and Authentication Site with the same name
- Problem inserting an entry with an IPv6 address into the Audit table
- Unable to configure IPv6 addresses to the Proxy Server
- Error message and wrong answer when entering "com" in the URL Lists search field
- "Out of memory" error when adding bulk file extensions
- NullPointerException in Dashboard when only one Policy Server
- Device Logging Policy: There was an option to delete a device logging policy which was set as default
- A Regular administrator could see all super admin users when setting a new logging policy to default
- When SNMPv2 was chosen and MIB Monitoring and TRAP Sending were disabled, all the other fields were enabled instead of disabled
- Enabling WCCP without Transparent mode raised no warning and these settings could be saved successfully
- User List did not work properly after LDAP users were imported for the first time
- When OS update was applied with the "Download & Install Now" option there was no status page after the install
- Some URL groups were not categorized correctly

- Support user had no ability to delete imported report
- Delete view in Log Views did not work
- Update table emptied when clicking Refresh
- Inconsistency in DLP validation with OR operator

Supported Appliances

The following SWG appliances are supported:

- SWG 3000/NG5000-S2 (IBM Model 3250 M3)
- SWG 3000/NG5000-S2 (IBM Model 3550 M4)
- TS-250 SWG
- SWG 5000 (IBM Model X3550 M3) *
- SWG 5000 (IBM Model X3550 M4)
- TS-500 SWG
- 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 11.6 requires a minimum of 4GB RAM. Appliances marked with an * 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 *SWG 11.6 Setup Guide.*

Notes:

SWG Installation Utility version 1.9.0.01 is required.

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

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.