Secure Web Gateway 11.7 Release Notes

Trustwave is pleased to announce the release of Secure Web Gateway version 11.7.

August 2015

Contents

New Features

Forensics

The new Forensics feature enables the collection of forensic data whenever the Malware Entrapment Engine blocks malware. A secure archive that includes transaction details, a description of the detected threats, and supporting files can be analyzed by your security experts for further investigation.

Support for OWA 2013

SWG 11.7 now fully supports Microsoft Outlook Web Access 2013.

Disaster Recovery Support

In SWG 11.7, you can dedicate an additional device as a Disaster Recovery Policy Server. In the event of failure of the Active Policy Server, you can manually switch between the previously active Policy Server and the Disaster Recovery Server. If required, you can also switch between the active Policy Server and the Disaster Recovery Server when both devices are up.

Disaster Recovery is used for Policy Servers deployed in separate locations. A High Availability deployment is used for redundant Policy Servers on the same network. To ensure that there is no single point of failure, we also recommend a crossover cable connection between high availability devices. If this is not possible, the Disaster Recovery solution should be considered.

IPv6-enabled FTP

SWG now supports an IPv6-enabled ftp proxy.

Hardware Security Module (HSM)

To safeguard and manage digital keys for strong authentication, and to enable performance improvement, SWG 11.7 enables you to integrate a certified Hardware Security Module (HSM) device into the security system topology.

For information on how to deploy an HSM device, contact Trustwave Support.

Other Enhancements

- SSL-related Improvements
- Native FTP now supports IPv6

Limitations and Known Issues

- Policy Server HA does not support IPv6
- WCCP with Generic Routing Encapsulation (GRE) is not supported with IPv6
- CSRs generated on HSM-enabled SWG can be signed only on Windows 2008 R2 servers or later. Earlier Windows versions will get an "Invalid algorithm" error.
- 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

- In some cases, the import of the SWG 11.6 upgrade FUP file failed
- The failover from StartTLS and LDAPS did not work properly
- The Audit Log in version 11.5 showed incorrectly when changes were made to Scanning Server Device Policies
- The Manager ICAP health check did not work on the scan module when HTTP role was disabled
- HTTP and ICAP services did not activate when the listening IPv4 address was set
- FTP over HTTP did not work with the cache disabled and in Bypass mode

- Blocking rules were not applied when uploading forbidden file types to a Microsoft OWA 2013 server
- Deleting a Web Log view did not work
- The URL Category column in the Web Log was not filled for category "Other"
- The passive Policy Server did not respond to the snmpd manager health check or the snmp server after configuring the snmp community to a different value than the default
- The SSH password did not change on the passive Policy Server after changing the password on the active Policy Server via the GUI

Supported Appliances

The following SWG appliances are supported:

- SWG 3000/NG5000-S2 (IBM Model 3550 M4)
- TS-250 SWG
- SWG 5000 (IBM Model X3550 M4)
- TS-500 SWG
- SWG 7100/NG8100-S1 (IBM Model HS23 7875)
- SWG 7080/NG8080-S1 (IBM Model HS23 7875)

Note: SWG 11.7 requires a minimum of 4GB 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 11.7 Setup Guide.*

Note:

SWG Installation Utility version 1.9.0.03 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

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 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.