Secure Web Gateway 11.7 Upgrade Release Notes

August 2015

Trustwave is pleased to announce that the upgrade path for Secure Web Gateway to version 11.7 is now available.

For more information on SWG 11.7, see the *Trustwave SWG 11.7 Release Notes*.

Contents

1   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.

2 Resolved Issues

- Web log data, Report data, and Report history are now retained on upgrade.

3 Limitations and Known Issues

- Upgrading Secure Web Service Hybrid cloud scanners requires assistance from Trustwave Support.
- Scanners require at least 4GB RAM to upgrade to version 11.7. Policy servers require at least 8GB RAM to upgrade to version 11.7.
- In a PKI environment, a generic certificate must be generated prior to upgrading/reconnecting scanners.
- Default and customized configuration settings are not overwritten by the upgrade process. This may result in settings that are not as secure as those provided by a standard installation of SWG 11.7.

4 Before You Start

Note the following:

- You can upgrade directly to SWG version 11.7 only from version 11.6.
- When upgrading from a version earlier than 11.6, incremental upgrades to version 11.6 are required first.
- SWG version 11.6 and later cannot be downgraded to versions prior to 11.6 due to the introduction of the TrustOS software platform. "Downgrade Policy Server to Previous Version" is therefore not available as a Policy Server option in the Devices tree.

  Reinstallation of a previous version prior to version 11.6 requires a backup of the Policy Server and Reports databases and a restore procedure. For more information, refer to the SWG Help or the *Management Console Reference Guide*.

- When upgrading from an SWG version earlier than version 11.5:

  - If the current version includes Websense or IBM URL Categorization, refer to Migrating from IBM and Websense URL Filtering Engines to the Trustwave URL Filtering Engine on page 3.

  - If Web log views include filters that refer to IBM or Websense categories, the migration process removes these filters from the view. As a result, the meaning of the filters might change. The user should review them to determine if any changes are required.
    For more information, refer to the section Migrating from IBM and Websense URL Filtering Engines to the Trustwave URL Filtering Engine on page 3.

  - If Audit log views include filters that refer to the Device IP column, the migration process removes these filters from the view. As a result, the meaning of the filters might change. The user should review them to determine if any changes are required.

4.1 Migrating from IBM and Websense URL Filtering Engines to the Trustwave URL Filtering Engine

Trustwave SWG versions 11.5 and later are offered with the Trustwave proprietary URL Filtering engine only. SWG is no longer reliant on third party vendors IBM and Websense for URL filtering engines.

For implementations that previously used IBM or Websense, Trustwave provides a migration utility that translates and maps IBM and Websense URL categories to Trustwave categories.

Note the following:

- Upgrading to SWG 11.7 from a system that used IBM or Websense URL filtering engines requires the **pre-installation** of a new valid Trustwave license, which includes the Trustwave URL categorization engine.

- The upgrade utility `migrate_url_filter_rules` is available in the Limited Shell, after installation of the relevant hotfix. Hotfix installation procedures are described in the hotfix Release Notes.

- Mapping from the IBM or Websense URL filtering engines to the Trustwave engine is performed automatically by the utility either on a 1-to-1 or 1-to-many basis.

- All changes, as well as warnings of URLs that cannot be mapped, are reported in an output file generated by the utility.

- Upgrading to SWG 11.7 from a system that used IBM or Websense URL filtering engines without running the migration tool will result in existing URL categorizations being lost.

5 Upgrading from Previous Versions

There are two upgrade methods:

- Upgrading by backing up all SWG data, installing the new version, and then restoring the data.
- Upgrading incrementally from the current version via the SWG console.

5.1 Upgrading from SWG Version 11.x to Version 11.7

When upgrading from a version earlier than 11.6, incremental upgrades to version 11.6 are required first.

To upgrade from version 11.0, 11.5 or 11.6:

1. Make sure that all Trustwave security updates are installed.
2. In the Policy Server, go to **Administration | Updates | Updates Management**.
3. In the Available Updates tab, click the icon for the update and select **Install Now**.
    The system will reboot. This may take some time.
4. Follow the steps on the displayed Status page.
5. When the restart is complete, login to the SWG console.
6. Go to **Administration | System Settings | SWG Devices**.
7. Right-click each relevant scanning device and select **Upgrade to PS version**.

6 High Availability and Disaster Recovery Policy Servers

The High Availability (HA) solution was designed for installations where the two Policy Servers were physically close, running on the same subnet, and had multiple connections between them.

If you are running HA between two different physical locations, we believe you would be better served by using the new Disaster Recovery (DR) solution and should consider switching.

The main differences between HA and DR features are that DR does not support a virtual IP nor does it support automatic failover. The advantage of DR is that it is a more robust solution that provides the required functionality should a disaster befall the primary Site. Manual failover in the DR environment is also more tightly controlled than in an HA environment, allowing a seamless transfer between Sites.

6.1 Upgrading to SWG Version 11.7 on a High Availability Setup (from version 11.0 and later)

1. Deactivate **High Availability** on the Passive Policy Server from the Active:
    a. Log into the Management Console on the Active Policy Server and go to **Administration | System Settings | SWG Devices**.
    b. Expand the node of the Active Policy Server and click **High Availability**.
    c. Click **Edit** and clear **Enable High Availability Policy Server**.
    d. Click **Save**.

2. Using the instructions in the section Upgrading from Previous Versions above, upgrade to SWG 11.7 on the Active Policy Server.
3. Install SWG 11.7 (clean installation) on the Passive Policy Server.
4. Activate the Passive Policy Server:
    a. Log into the Management Console on the Active Policy Server and go to **Administration | System Settings | SWG Devices**.
    b. Expand the node of the Active Policy Server and click **High Availability**.
    c. Click **Edit** and select **Enable High Availability Policy Server**.
    d. Click **Save**.

7 Documentation

For documentation available online, go to:
https://www.trustwave.com/support/Secure-Web-Gateway/Documentation.asp

Legal Notice

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.