

Secure Web Gateway 12.0 Upgrade Release Notes

September 2018

Trustwave is pleased to announce that the upgrade path for Secure Web Gateway to version 12.0 is now available.

For more information, see the *Trustwave SWG 12.0 Release Notes*.

Contents

1	Supported Appliances	2
2	Limitations and Known Issues	2
3	Before You Start	3
4	Upgrading from Previous Versions.....	3
5	High Availability and Disaster Recovery Policy Servers.....	4
6	Documentation.....	4

1 Supported Appliances

The following SWG appliances are supported:

- TS-5000 SWG BladeCenter
- 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 12.0 requires a minimum of 8GB RAM. 16GB RAM is recommended. To purchase additional memory, contact your Trustwave Channel Partner/Account Manager.



Note about Ethernet ports in the 1Gb version of the TS-5000 SWG BladeCenter: In the default configuration, the chassis is delivered with 3 switches; A 10GB switch connected to ETH0 of each blade server, a 1GB switch connected to ETH1, and another 1GB switch connected to ETH2. If the relevant chassis does not include the 10GB switch, ETH1 (and not ETH0) will be configured as the main port.

2 Limitations and Known Issues

- Upgrading Secure Web Service Hybrid cloud scanners requires assistance from Trustwave Support.
- Scanners require at least 8GB RAM to upgrade to version 12.0. Policy servers require at least 8GB RAM to upgrade to version 12.0.
- 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 12.0.

3 Before You Start

Note the following:

- You can upgrade directly to SWG version 12.0 only from version 11.8.2.
- When upgrading from a version earlier than 11.8.2, incremental upgrades to version 11.8.2 are required first.
 - You can upgrade to 11.8.2 from 11.8.0 or 11.7.2 only
 - You can upgrade to 11.8.0 from 11.7.2 only
 - You can upgrade to 11.7.2 from 11.7.0 or 11.7.1 only
- Upgrading to SWG 12.0 will fail if any Admin passwords are encrypted using MD5. A list of these Admins is reported in the System Log. These passwords must be manually changed by a super Admin before restarting the upgrade process.

4 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 from the backup.
- Upgrading incrementally from the current version via the SWG Web UI.

4.1 Upgrading from SWG Version 11.x to Version 12.0

When upgrading from a version earlier than 11.8.2, incremental upgrades to version 11.8.2 are required first. The upgrade path is described in Section 3 above.

To upgrade from a previous version:

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 Web UI.
6. Go to **Administration | System Settings | SWG Devices**.
7. Make sure you have the latest Automatic Hotfix (AHF) installed.
Go to **Administration | Updates | Updates Management** and click the **Retrieve Updates** button to install the latest update.
8. Right-click each relevant scanning device and select **Upgrade to PS version**.

5 High Availability and Disaster Recovery Policy Servers

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

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.

5.1 Upgrading to SWG Version 12.0 on a High Availability or Disaster Recovery Setup

1. Deactivate **High Availability** on the Passive Policy Server from the Active:
 - a. Log into the SWG Web UI on the Active Policy Server and go to **Administration | System Settings | SWG Devices**.
 - b. Expand the **Management Devices Group**.
 - c. Right-click the passive policy server and select **Delete Device**.
 - d. Click **Save** and **Commit**.
2. Using the instructions in the section Upgrading from Previous Versions above, upgrade to SWG 12.0 on the previously active Policy Server.

Make sure you have the latest Automatic Hotfix (AHF) installed. Go to **Administration | Updates | Updates Management** and click the **Retrieve Updates** button to install the latest update.
3. Install SWG 12.0 (clean installation) on the previously passive Policy Server.
4. Activate the previously passive Policy Server:
 - a. Log into the SWG Web UI on the Active Policy Server and go to **Administration | System Settings | SWG Devices**.
 - b. Right-click **Management Devices Group** and select **Add HA/DR Device**.
 - c. Click **Save** and **Commit**.

6 Documentation

For documentation available online, go to:

<https://www.trustwave.com/support/Secure-Web-Gateway/Documentation.asp>

Legal Notice

Copyright © 2018 Trustwave Holdings, Inc.

All rights reserved. This document is protected by copyright and any distribution, reproduction, copying, or decompilation is strictly prohibited without the prior written consent of Trustwave. No part of this document may be reproduced in any form or by any means without the prior written authorization of Trustwave. 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 helps businesses fight cybercrime, protect data and reduce security risk. With cloud and managed security services, integrated technologies and a team of security experts, ethical hackers and researchers, Trustwave enables businesses to transform the way they manage their information security and compliance programs. More than 2.7 million businesses are enrolled in the Trustwave TrustKeeper® cloud platform, through which Trustwave delivers automated, efficient and cost-effective threat, vulnerability and compliance management. Trustwave is a privately held company, headquartered in Chicago, with customers in 96 countries.

For more information, visit <https://www.trustwave.com>.