MAINTENANCE RELEASE NOTES

Secure Web Gateway 12.0.1

December 2019

Trustwave is pleased to announce the availability of Maintenance Release 12.0.1 for Secure Web Gateway version 12.0.

Very Important:

- This update can be installed over SWG 11.8.3 and 12.0.0 only.
- If you are upgrading from 12.0.0 version – please make sure that Runtime Hotfix 12.0.0.RHF02 is already installed
- For high availability or disaster recovery environments, high availability needs to be unset and the release must be installed separately on each Policy Server. See How to Install This Release.
- After installing and linking a new 12.0 scanner, the upgrade to this release must be performed immediately.
- Scanner appliances with installed bypass adaptors will automatically switch to bypass mode after upgrade and will not scan traffic. To resolve the issue, run the config_hardware command from the limited shell on each scanner appliance and restart the appliance.
- In some cases, Page Trickling's .mp4 file type exclusion may be missing from the configuration. To prevent streaming issues, please re-add .mp4 to the exclusion list found under Administration -> Scanning Options -> Enable Status Page -> Activate -> Unless.
- **Rollback** to a previous version is enabled in this minor release.
- **A reboot is required** after installation of this release.
- This release includes all previous hotfixes to 12.0.

How to Install This Release

1. The maintenance release will appear in the Available Updates window. If it does not appear immediately, click the **Retrieve Updates** button.
2. Select the release from the list and click **Install Update**. Once the release has been installed, it will move to the Installed Updates tab.
3. When the restart is complete, log in to the SWG Web UI.
4. Go to Administration | System Settings | SWG Devices.
5. Right-click each relevant scanning device and select **Upgrade to PS version**.
6. For high availability or disaster recovery environments:
    a. Unset the High Availability environment into separate Policy Servers.
    b. Install the update onto each Policy Server.
    c. Run **#make_passive** on the passive Policy Server.
    d. Reconnect the Policy Servers into High Availability or Disaster Recovery mode.
7. Reboot after installation.

New Features in SWG 12.0.1

This list only includes the items new in 12.0.1. For items introduced in SWG 12.0, see the Release Notes for 12.0.

Extended Categorization Services

If the SWG scanner cannot categorize the transaction URL, it can optionally send an additional request to a dedicated portal service to perform an additional categorization check.

Cloud Services Credentials

Extended Categorization Services require you to enter a credential on the page Administration > System Settings > Scanning > Scanning Options. These credentials can only be entered once.

The same credentials are used for the Sandbox service introduced in release 12.0.0. Credential entry for Sandbox has been moved to the Scanning Options page.

Updated McAfee Anti-Virus Engine

An updated McAfee Anti-Virus (AV) engine is included in this release. For customers currently using McAfee AV, ***please upgrade now*** to ensure your continued receipt of AV signature updates.

Supported Appliances

See the Hardware Support Matrix document available on the SWG Documentation web page for the latest information about supported appliances.

The following SWG appliances are supported:

- TS-5000 SWG BladeCenter
- TS-250 SWG
- 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.

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 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 three 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 headquartered in Chicago, with customers in 96 countries. For more information about Trustwave, visit https://www.trustwave.com.