Mobile Security Client 2.4 Release Notes for SWG Enterprise

August 2016

Trustwave is pleased to announce the availability of Mobile Security Client version 2.4.

Notes

- This update can be installed on MSC software version 2.3 only.
- This update is for Secure Web Gateway version 11.8 and is visible only when SWG Cloud Scanners are in use.

Supported Operating Systems and Browsers

Note: Only the operating system/browser types defined in the table are officially supported by Trustwave.
Mobile Security Client will also work with other browser types and programs that can be configured to make use of the Windows Internet connection settings or a Proxy Auto.

O/S Platform	Internet Explorer	Edge	Safari	Firefox	Chrome
Windows 7	10,11		n/a	47.01	51.0.2704
Windows 8	11		n/a	47.01	51.0.2704
Windows 8.1	11		n/a	47.01	51.0.2704
Windows 10	IE is not supported on Windows 10	20.10240	n/a	47.01	51.0.2704
Mac OS X Mountain Lion	n/a		6.2.8	47.01	49.0.2623
Mac OS X Mavericks	n/a		9.1.1	47.01	51.0.2704
Mac OS X Yosemite	n/a		9.1.1	47.01	51.0.2704
Mac OS X El Capitan	n/a		9.1.1	47.01	51.0.2704

How to Install this Update on Secure Web Gateway

The following instructions describe installation in Secure Web Gateway deployments.

1. In the Management Console, navigate to **Administration | Updates and Upgrades | Management**.
2. In the Available Updates list, select the Maintenance Update and click **Import Update**.

   After the Maintenance Update has been installed, the Installed Updates tab will open.
3. Unless configured differently, existing installed MSC clients will automatically update to the most recent version according to administrative settings. New clients can be installed in the normal way.

Modifications and Enhancements

- This update delivers new features and enhancements and also provides bug fixes.
- The new structure and features include the MSCProxy component that prevents browsing to HTTPS sites when no scanner connection is established and admin has configured the client to fail-close or to Hotel mode.
- By default, the grace period for the client starts whenever the computer wakes from sleep, exits from hibernate mode, exits from screensaver, unlocks, or on login to the computer. Admin can configure the Grace period to reset only on Log-in.

Bug Fixes

- Fixed issue where Safari did not refresh the PAC it was working with unless a major change such as a path change was detected. To overcome this, enforcement is disabled when the PAC changes to clear definitions and is then re-enabled.

Limitations and Known Issues

- MSC for SWG Enterprise does not support multilingual environments and settings.
- Microsoft Edge browser is not fully supported and users should upgrade to Windows 10 Anniversary Edition.
- MSC and some Sophos Web Protection services do not coexist well on the same machine. These are Sophos Web Control, Sophos Web Filter, Sophos Web Intelligence Service and Sophos Network Threat Protection.
- When using MSC with a PAC file in Internet Explorer, trusted URLs with non-ascii characters in the path are not bypassed and are sent to the scanner.
- In SWG Cloud, the MSC client cannot run on a pure Japanese user account defined on LDAP, and MSC will not function if pushed to a Mac.
- MSC Uninstall warning text does not support multilingual messages.
- In some user configuration scenarios in Windows 10, MSC PAC enforcement loses synchronization with the registry and will not work correctly.

- When using MSC with a PAC file in Microsoft Edge, HTTPS traffic is not diverted to SWG scanners:
  - when fail-open or Hotel-mode are configured for the MSC,

    and
  - when the installed Windows 10 version is earlier than the Anniversary edition release.

  Users should therefore update their Windows 10 to the Anniversary edition.

Documentation

The following documentation is also available for MSC version 2.4: *Mobile Security Client Administrator Guide*.

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, visit https://www.trustwave.com.