



 **Trustwave**[®]
Smart security on demand

Mobile Security Client
Version 2.3
Administrator Guide

Legal Notice

Copyright © 2014 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: support@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.

Revision History

Version	Date	Changes
1.0	September 2012	Version Release 2.0
2.0	December 2012	Version Release 2.1
3.0	November 2013	Version Release 2.2
4.0	November 2014	Version Release 2.3

Formatting Conventions

This manual uses the following formatting conventions to denote specific information.

Formats and Symbols	Meaning
Blue Underline	A blue underline indicates a Web site or e-mail address.
Bold	Bold text denotes UI control and names such as commands, menu items, tab and field names, button and checkbox names, window and dialog box names, and areas of windows or dialog boxes.
Code	Text in Courier New 9 pt in blue indicates computer code or information at a command line.
Italics	Italics denotes the name of a published work, the current document, name of another document, text emphasis, to introduce a new term, and path names.
[Square brackets]	Square brackets indicate a placeholder for values and expressions.

Notes, Tips, and Cautions



Note: This symbol indicates information that applies to the task at hand.



Tip: This symbol denotes a suggestion for a better or more productive way to use the product.



Caution: This symbol highlights a warning against using the software in an unintended manner.



Question: This symbol indicates a question that the reader should consider.

About this Guide

This guide is intended to help system administrators with the installation and operation of the Trustwave Mobile Security (MSC) Client software. In use the software should be self-explanatory or invisible depending on how the Administrator has configured it. Consequently there is no actual end-user (consumer) guide for the MSC.

The MSC is used with both **Secure Web Gateway (SWG) v10.2** and later and **Web Filter (WFR) v 5.0** and later. When there is a difference in MSC functionality or behavior when used with SWG vs. WFR, this will be highlighted. When the server side of the product deployment is being referred to this will be referred to in capitalized form as follows: **Server**.

Table of Contents

Legal Notice	ii
Trademarks	ii
Revision History	ii
Formatting Conventions	iii
Notes, Tips, and Cautions	iii
About this Guide	iv
Table of Contents	v
1 Introduction	7
1.1 What is the Mobile Security Client?	7
1.2 Terminology	7
2 Client Architecture	7
2.1 Functionality	7
2.2 Components and Outline Operation	8
2.3 Local IP Port Usage	9
2.4 User Identification	9
2.4.1 Simple Client Mode (WFR Only)	9
2.4.2 Individual User Certificates	10
2.4.3 User Certificate Not Present (SWG v11.0 and later and MSC v2.1 and later only)	10
2.5 On/Off Premise Behavior	10
3 Supported Operating System and Browsers	11
4 Installation and Removal	11
4.1 Client Settings at Install	11
4.2 Client Deployment	12
4.3 Microsoft Windows – Manual Installation/Removal	12
4.3.1 System Requirements	12
4.3.2 Install Procedure for Windows	12
4.3.3 Uninstall Procedure for Windows	13
4.4 Apple Mac OSX – Manual Installation/Removal	14
4.4.1 System Requirements	14
4.4.2 Install Procedure for Mac	14
4.4.3 Uninstall Procedure for Mac	15
4.5 Client Tamper Resistance	15

5 Server Selection	15
<hr/>	
5.1 Initial start-up	15
5.2 Auto-tuning.....	16
5.3 Failover	16
6 PAC File	16
<hr/>	
6.1 Structure	16
6.1.1 Bypass URLs	16
6.1.2 Non-Routable Networks.....	16
6.1.3 On/Off Premise	17
6.1.4 On-Premise PAC File Option (SWG Only)	17
6.2 Connectivity Management	17
6.2.1 Server not found (WFR Only)	17
6.2.2 Server Not Found (SWG v11.0 and later with MSC v2.1 and later only)	17
6.3 Enforcement.....	18
7 Tray Icon Menu Functions	18
<hr/>	
7.1 MSC Status	18
7.2 Options.....	19
7.2.1 Enable/Disable.....	19
7.2.2 About.....	19
7.3 Hiding System Icon Tray (WFR Only).....	19
8 Automatic Updates	20
<hr/>	
8.1 MSC Configuration Updates	20
8.2 On-going MSC Code Updates	20
8.2.1 New Granular Code Updates (SWG v11.0 and later with MSC v2.1 and later only)	20
<hr/>	

1 Introduction

1.1 What is the Mobile Security Client?

The Trustwave Mobile Security Client (MSC) is used by Trustwave Secure Web Gateway and Trustwave Web Filter to perform Internet traffic scanning and filtering of end-user mobile PCs located outside of the organization. This product requires either an SWG or Web Filter dedicated to scanning/filtering mobile workstations, and uses certificates to validate end-users before granting them Internet access based on their profiles.



Note: When used with the Web Filter product, user certificates are optional.

1.2 Terminology

The following terms are used throughout this guide:

Server	Trustwave SWG Cloud Scanner, or Trustwave WF Mobile Server
MSC	Mobile Security Client; works with both SWG and WFR products
SWG	Trustwave Secure Web Gateway product
WFR or WF	Trustwave Web Filter product
PC	Personal computer; refers to both MS Windows and Apple Mac based systems
PAC	Proxy Auto Configuration file, as used by Web browsers and some applications
Mac OS X	Apple Macintosh ("Mac") operating system

2 Client Architecture

2.1 Functionality

The MSC performs the following functions:

- Re-directs Web traffic from a user's PC to a Server component (Cloud Scanner for SWG, Mobile Server for WFR).
- Selects the most appropriate server and deals with failover between Servers.
- Secures communications between the client and the Servers (ensures privacy).

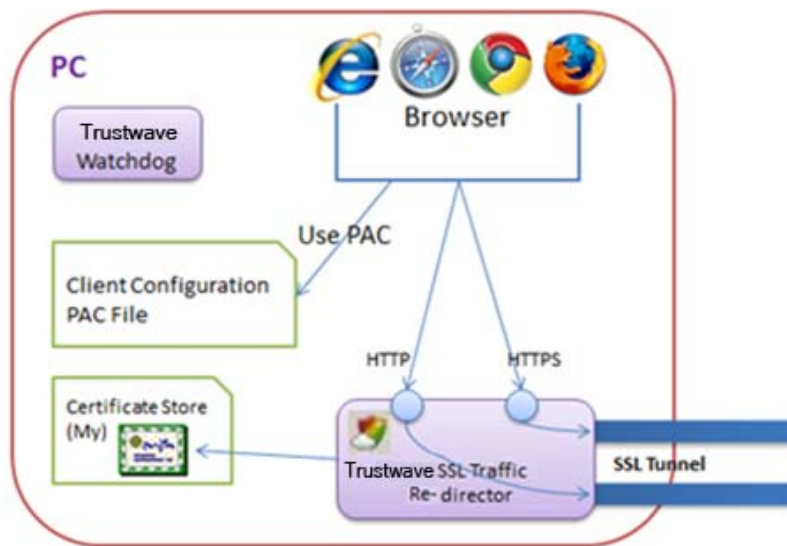
- Identifies and authenticates the user and machine using certificates (or login details on WFR).
- Enforces the MSC and web browser configuration (tamper resistance).

2.2 Components and Outline Operation

The MSC consists of a number of components installed on the mobile machine:

- Trustwave SSL Traffic Re-director client to supply the secured tunnel to the Servers.
- Configuration files indicating the Servers' information (e.g. IP addresses and priorities).
- Client Certificate used to authenticate with the Servers. Note: User certificates are not required when installing the MSC in Simple Client mode in a Web Filter deployment.
- References to existing or external resources such as the User Certificate and the PAC file to be used.
- Watchdog process to enforce persistent browser/PAC file configuration and client operation, and to perform activity checks, configuration updates and client code updates.

This client architecture is shown in the diagram below:



In operation, the MSC acts as a mini local proxy, listening on "Local Client" HTTP/HTTPS ports which determine where the browser must direct its traffic. The redirection is handled by a PAC file that is either deployed as part of the MSC installer package (default) or by the customer administrator.

2.3 Local IP Port Usage

The Trustwave SSL Traffic Re-director listens to several local ports as described in the following table. Refer to the [MSC Architecture](#) diagram when referring to the table.



Note: All Local Client ports are configurable.

Local Client IP Port #	Purpose
(Assigned dynamically)	The Control port used by the Trustwave Watchdog for configuration and binary updates as well as heartbeat when configured.
HTTP1	Used by the browser to redirect HTTP traffic through a specific Server #1 for scanning purposes. The browser redirects HTTPS through this port if HTTPS is not configured.
HTTPS1	Used by the browser to redirect HTTPS traffic through a specific Server #1 for scanning purposes.
HTTP2	Used by the browser to redirect HTTP traffic through a specific Server #2 for scanning purposes. The browser redirects HTTPS through this port if HTTPS is not configured.
HTTPS2	Used by the browser to redirect HTTPS traffic through a specific Server #2 for scanning purposes.

The Administrator should define HTTP# and HTTPS# ports for each configured server.



Note: A Server can also be a load balancer, hiding several 'real' Servers behind it.

2.4 User Identification

2.4.1 Simple Client Mode (WFR Only)

If the MSC is installed in Simple Client Mode, user identification is based on collecting details from the user login information. These are then shared with the server side and used to identify the user in logs and to apply acceptable use policy. The user's Web traffic is automatically encrypted by the client.



Note: It is possible to have a mixed deployment, where some PCs use Simple Client Mode and some use User Certificates.

MSC also supports Identification Only mode, where the policy server acts as the Certificate Authority for the server and generic user certificates only. There is no distribution of user certificates - identity information is automatically gathered from the user's machine for the currently logged in user.

2.4.2 Individual User Certificates

If user certificates are deployed, a dedicated client certificate is used to both identify and encrypt the user's traffic. A Certificate Authority that is known to the Server must sign the client certificate so that an SSL tunnel can be established between the Trustwave SSL Traffic Re-director and the server.

The client certificate resides in the end-user certificate store (Personal Certificate Store on Windows Login, KeyChain on Mac systems). Its attributes must correlate with the MSC configuration so that the client will be able to find and use it.

2.4.3 User Certificate Not Present (SWG v11.0 and later and MSC v2.1 and later only)

If no User Certificate is presented, the MSC is able to use a built-in generic certificate tied to the SWG Policy Server. The administrator can then choose which SWG Security Policy should be used to control Web access. This provides flexibility in the way that the MS is deployed, for example:

- Block all Web access until a User Certificate is provided.
- Allow limited Web access until a user certificate is provided – Can be used for quick deployment where user identification is not required, e.g. pilot, proof of concept, or test environment scenarios.

Be aware that using the generic certificate means that there is no user identification information in the SWG logs or reports. Trustwave recommends using individual user certificates.

2.5 On/Off Premise Behavior

The MSC has the ability to behave differently when it detects it is on premise (within the organization) or off premise (outside the organization). In the Policy Server (see **Administration | Cloud | Configuration | Proxies (On-premise)**) an On-Premise/Off-Premise indicator can be set which consists of an IP hostname that can be resolved to a pre-defined value when the MSC is on premise (but not when off premise).

It is then possible for the client when on-premise to avoid traffic redirection altogether. This grants the on premise security services the ability to process the end-user traffic (e.g. transparent proxy). For the SWG another option is to redirect the traffic to a certain set of proxies when on premise (implicit proxy). In this case the on-premise proxies are defined in the SWG Server configuration alongside the On/Off-Premise Indicator.

See also Section 6.1.4 On-Premise PAC File Option (SWG Only).

This behavior is configured in the Policy Servers of the respective WFR or SWG products being used.



Tip: For further details when using the MSC with SWG or WFR, refer to the *Trustwave SWG Hybrid Deployment Guide*.

3 Supported Operating System and Browsers

O/S Platform	Internet Explorer	Safari	Firefox	Chrome
Windows 7	9,11	n/a	29	35
Windows 8	10	n/a	29	35
Windows 8.1	11	n/a	29	35
Mac OS X Lion	n/a	6.1.3	28	35
Mac OS X Mountain Lion	n/a	6.1.3	29	35
Mac OS X Mavericks	n/a	7.0.3	29	35



Note: Only the operating system/browser types defined in the table above 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.

4 Installation and Removal

4.1 Client Settings at Install

The installation process implements the MSC components and sets an initial default configuration as defined on the Server. System settings (Internet Properties in MS Windows) are automatically adjusted to use "auto configuration script" and the URL location of the MSC Proxy Auto Configuration (PAC) file is set. Browsers and other applications that use the system settings will automatically use the PAC file. Other supported browser types will have their network settings adjusted directly by the MSC to point to the same PAC file.

To help mitigate tampering, this setting of network configuration happens both when MSC is started, and:

- For Windows: periodically while MSC is running
- For Mac: immediately whenever there are proxy configuration changes

4.2 Client Deployment

Initial installation/deployment of the MSC software can be managed as follows:

- Internal distribution (Trustwave SWG product Only)

When using the Trustwave SWG, the client can be distributed by using the built-in email feature of the SWG Policy Server and then manual installation by the end-user. A customizable email contains a download link and instructions for installing the MSC. The download location is chosen by the administrator and can be placed on an internal shared directory or in a Web server requiring a user/password or FTP server or even sent by email. This method requires manual MSC installation (see below) and is effective for small/medium size and proof of concept deployments.

- External software management system

In a Microsoft environment, an external software management system, such as Microsoft Group Policy Objects, can be used to deploy the MSC. The administrator makes the MSC install package available to the GPO system and end-user systems are installed at domain login time. A silent install option (see below) is also available. In a Mac OSX environment, the equivalent software distribution system, e.g. Casper Suite or Apple Remote Desktop Management could be used. Alternatively, the client code could be built into a master image of the client machines.

Subsequent MSC updates are handled automatically; See Section 8.2 On-going MSC Code Updates.



Caution: The MSC installer package for Windows is provided as an .exe file. If an .msi installer type is required then this can be achieved by using a third party .exe to .msi conversion tool.

Trustwave makes no representations or warranties of any nature regarding the third party tools/products referenced herein. Your use of such third party tools/products is entirely at your own risk, and you agree Trustwave shall have no liability resulting therefrom.

4.3 Microsoft Windows – Manual Installation/Removal

4.3.1 System Requirements

- See the system requirements table in Section 3, Supported Operating System and Browsers for operating system and browser versions.
- All local ports on the Windows PC should be available for the MSC to use.
- Installation is performed under Administrator privileges.

4.3.2 Install Procedure for Windows



Note: Only the administrator of the end-user machine can install the MSC. Silent installation can be achieved by entering the command line and executing the MSC installer with the "/S" flag. Otherwise, an interactive installation will begin.

To install the Windows client interactively:

1. Double-click the MSC installer.
2. Follow the installer dialogue.

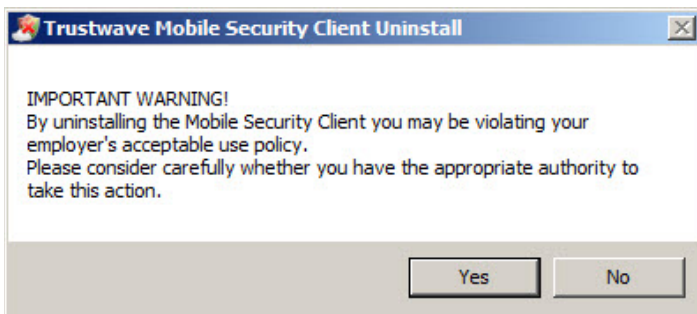


3. Accept the License Agreement.
4. Restart any running browsers after the installation finishes.

4.3.3 Uninstall Procedure for Windows

To uninstall the Windows client:

1. Open **Add / Remove Program** or **Programs and Features**, depending on the Windows OS version.
2. Choose to uninstall the Trustwave Mobile Security Client.
3. Follow the uninstall instructions.
4. Depending on the server side settings (SWG: Cloud Configuration Tab – "Enable Client Uninstall Warning") a customizable Uninstall Warning dialogue box may appear.



5. To continue the uninstall process select **Yes**, or to abort the process select **No**.

4.4 Apple Mac OSX – Manual Installation/Removal

4.4.1 System Requirements

- See the system requirements table in Section 3 for operating system and browser versions.
- All local ports on the Mac PC should be available for the MSC to use.
- Installation is performed under Administrator privileges.

4.4.2 Install Procedure for Mac



Note: Only a user with root privileges can install MSC.

To install the Mac OSX client:

1. Double-click the compressed MSC installer (suffixed with .tgz)
2. Double-click the MSC installer (suffixed with .mpkg)



Note: The Gatekeeper feature in OS X can block application downloads that are not from an identified source. In this case, a message will open advising that the installation file is from an unidentified developer.

1. Close the message.
 2. Right-click the MSC .mpkg installer file and click **Open** in the context menu.
A confirmation message will open.
 3. Click **Open** in the message to allow the file to run.
-

3. Follow the installer instructions.
4. Accept the License Agreement.
5. Restart the machine once the installation completes.



Tip: For further details when using the MSC with SWG or WFR, refer to the *Trustwave SWG Hybrid Deployment Guide* or the *Trustwave Web Filter User Guide for Mobile Security Client* respectively.

4.4.3 Uninstall Procedure for Mac

To uninstall the Mac client:

1. Search for MSCUninstaller in Spotlight and double-click on it (as an application).
2. Follow the uninstall instructions.
3. Depending on the server side settings (SWG: Cloud Configuration Tab – "Enable Client Uninstall Warning"), a customizable Uninstall Warning dialogue box may open.
4. To continue the uninstall process select **Yes**. To abort the process select **No**.

4.5 Client Tamper Resistance

Trustwave recommends that the end-user does not have local administrative rights. In this situation the MSC can be locked down. However, in some situations a full lock down is not possible and it becomes nearly impossible to prevent end-users from tampering with a system. It is however possible to take some pragmatic measures to make the configuration persistent. The MSC performs the following tamper-resistant actions:

- Every 15 seconds the client checks for changes to the Proxy settings on the PC and returns them to the original values.
- If a user is able to stop the MSC client process, it will automatically re-start in about 10 seconds.
- Every hour the PAC file configuration is refreshed using the official copy (see also section 6.3 below).
- If the user attempts to remove the client through the uninstall process, a customizable warning banner is presented.

5 Server Selection

The following section explains how the MSC optimizes the connection to the Server side to help ensure the best Web browsing performance and reliability are achieved with the available Server deployment.

5.1 Initial start-up

On start-up the MSC uses its default Server while it tests the network latency and reliability for each available Server listed in its configuration file. A selection is then made based on the lowest network latency (i.e. fastest connection) with reliable connectivity. The user can browse normally from start-up with full protection of the Server security policy while this optimization takes place.

5.2 Auto-tuning

Further latency tests are performed periodically to check for a better connection. If, through changing network conditions for example, a significantly better Server connection becomes available, the MSC will switch to that Server. The selection mechanism introduces damping to prevent unnecessary switching between Servers.

The MSC builds a reputation for each Server based on the reliability of its connectivity as seen in the network latency measurements. This evaluation is factored into the server selection process. If connection to the Server is unreliable, it is marked as unavailable until such time as the test results show its reputation has improved sufficiently that it can be reused.

5.3 Failover

In addition to auto-tuning, keep-alive tests are performed. If the currently used server becomes unresponsive (unavailable), the MSC will failover to the next best Server. If the Server subsequently becomes available again this will be reflected in the latency tests.

6 PAC File

The Proxy Auto-Configuration (PAC) file is used by browsers to determine which proxy to use for a given URL request. The PAC file directs the browser to use the locally running Trustwave SSL Traffic Redirector as its proxy and by this redirects Web traffic to the server.

6.1 Structure

The MSC PAC file operates under several conditions, all aimed at avoiding traffic redirection. If none of the conditions are met, traffic is redirected to the configured Servers.

6.1.1 Bypass URLs

The administrator can define a list of URLs to be bypassed by the MSC. In such a case, if the PAC file is asked for a proxy to one of the URLs in the list, the PAC file will return the "DIRECT" directive requesting the browser to avoid using a proxy for that URL.

6.1.2 Non-Routable Networks

According to IPv4 standards (see RFC5735 and RFC1918) there are certain network ranges that can only be defined in a local network. That is, if someone tries to access an address within one of those network ranges, it can't be found on the Internet but can be found on the local network.

Hence, if the PAC file detects the requested URL address is within one of those non-routable networks, it will return the "DIRECT" directive requesting the browser to avoid using a proxy for this URL.

6.1.3 On/Off Premise

The MSC might be expected to work differently when the end-user is on premise (e.g. organization HQ) and there are already security servers within the local network. In such a case, there is no need for the traffic to be redirected to the Servers (WF Mobile Server or SWG Cloud Scanner). The PAC file can detect such a scenario, given the right configuration, and either return the "DIRECT" directive requesting the browser to avoid using an explicit proxy, or return the on premise proxy addresses as the proxy servers through which traffic should be redirected.

6.1.4 On-Premise PAC File Option (SWG Only)

As of MSC v2.1 and SWG V11.0, it is possible for the MSC to use a local PAC file when on-premise instead of the SWG provided version. This is useful in complex networks with many proxy bypass and redirection requirements. Set the option and the PAC file location in the SWG Policy Server (**Administration | Cloud | Proxies (On-premise)**).

6.2 Connectivity Management

6.2.1 Server not found (WFR Only)

The administrator can define how the MSC behaves in the event that a WF Mobile Server cannot be found. The options are to:

- Prevent Internet access: The "DIRECT" directive won't be added to the end of the proxy servers (Server) list. Hence, if no Server is available, the browser will fail to complete the request.
- Allow direct access to the Internet (the default): Where the PAC file will always add "DIRECT" to the end of the proxy servers list. This way, if proxy servers (Servers) are unavailable for any reason the user can still surf the Web. This is required, for example, to negotiate Wi-Fi billing systems in Airports and Hotels.

6.2.2 Server Not Found (SWG v11.0 and later with MSC v2.1 and later only)

The administrator can define how the MSC behaves in the event that a SWG Cloud Scanner cannot be found. The options are to:

- Disable Web access
- Enable "Hotel Mode" for a period of time (default 5 minutes)
- Allow direct Web access.

Hotel mode allows the user to negotiate a hotel style billing system that controls access via a local firewall to the Internet. Once account details have been established (and payment made in some cases) the MSC will continue to look for a Cloud Scanner. If none is found within the timeout period, the MSC will disable Web access.

This flexibility allows the administrator to tune MSC behavior according to company policy.

6.3 Enforcement

If the administrator chooses the MSC to enforce the PAC file on the browsers, the MSC will define its PAC file as the one to be used by all supported browsers. It will then make sure this configuration is not changed in any way.



Note: Browser behavior varies. However, they usually load the PAC file upon startup. Hence, if a browser is already running and using a different PAC file or none at all, it will only use the new PAC file once it has been restarted.

7 Tray Icon Menu Functions

7.1 MSC Status

The tray icon indicates MSC status. Possible states are:



Enabled – normal operation.



Disabled



Connection pending – client is attempting to connect to the server.

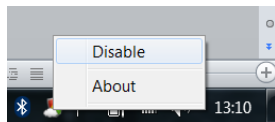



Error condition

7.2 Options

7.2.1 Enable/Disable

The administrator can configure, on the Server side, an option that allows specified trusted end-users to temporarily disable the re-direction of Web traffic. Simply right-click the tray icon and select **Disable**.



The disabled icon  will be displayed as a reminder.


Re-direction configuration will be re-enabled when any of the following events occur:

- The user right-clicks the icon and selects **Enable**.
- The user is 'locked out' through the PC being dormant.
- The user logs out.
- The machine is shutdown.

7.2.2 About

The about screen allows the end-user to see the product version and copyright notice. It also provides a way to collect support information for troubleshooting purposes.

7.3 Hiding System Icon Tray (WFR Only)

It is possible, from the WFR Server side, to set configuration so that the MSC system tray icon , which normally indicates the status of the MSC, is hidden from view. In the event that status information is needed, the administrator will need to instruct the user how to collect support information manually.

8 Automatic Updates

8.1 MSC Configuration Updates

Checks for MSC configuration updates are performed once per hour. When a configuration update is detected, a fresh copy is downloaded and applied, and the MSC begins utilizing the new configuration immediately; this is all transparent to the end-user.

The MSC is capable of handling most configuration changes automatically as long as there are no certificate authority-related changes and at least one Server IP address remains unchanged so that the new configuration can be obtained. However, browsers will need to be restarted in order to use an updated PAC file.

When a major new MSC version is made available, the existing (i.e. older) MSC cannot update its configuration until it too has been upgraded to the latest version.

8.2 On-going MSC Code Updates

Once installed, the MSC client code (binary) is updated automatically (Note: Applies to Trustwave SWG versions 10.2 and Trustwave MSC 2.0.1 onward) when a new version is made available by the administrator from the Server side. The MSC client checks once per hour for code updates and if a newer version is available it will automatically download and execute it.



Note: Upgrade instructions are made available with new versions of the MSC code.

8.2.1 New Granular Code Updates (SWG v11.0 and later with MSC v2.1 and later only)

Automatic upgrades of the MSC can be switched on or off at a global level and also controlled by group membership. This allows for a controlled roll-out of new MSC versions to pilot groups before committing to a full roll-out

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>.