



M86 Security is now part of Trustwave. <https://www.trustwave.com/acquisition/>

# Mobile Security Client (MSC) Administrator Guide

Release 2.0.1 Manual Version 2.1

## Confidentiality, Copyright and Disclaimer

© Copyright 2012. Trustwave Holdings. All rights reserved.

This document may not, in whole or in part, be copied, published or reproduced without prior written consent from Trustwave. Every effort has been made to ensure the accuracy of the content contained in this document. Such content is provided “as is” without warranty of any kind. Trustwave disclaims all warranties and conditions with regard to this content, including all expressed or implied warranties and conditions of merchantability, and fitness for a particular purpose. The company shall not under any circumstance be liable for any errors or damages of any kind (including but not limited to compensatory, special, indirect or consequential damages) in connection with the document’s contents. Trustwave, the Trustwave logo, Trustwave-branded products, M86 Security, the M86 Security logo and M86-branded products are registered trademarks under license by Trustwave. All other product and company names mentioned herein are trademarks or registered trademarks of their respective companies. All rights reserved.

## Trustwave Security Client Administrator Guide

© 2012 Trustwave

All rights reserved.

70 West Madison Street, Chicago, IL 60602, United States

All text and figures included in this publication are the exclusive property of Trustwave. This document may not, in whole or in part, be copied, published or reproduced without prior written consent from Trustwave. Every effort has been made to ensure the accuracy of the content contained in this document. Such content is provided "as is" without warranty of any kind. Trustwave disclaims all warranties and conditions with regard to this content, including all expressed or implied warranties and conditions of merchantability, and fitness for a particular purpose. The company shall not under any circumstance be liable for any errors or damages of any kind (including but not limited to compensatory, special, indirect or consequential damages) in connection with the document's contents. Any information in this document is subject to change without notice. Trustwave, Trustwave logo, Trustwave-branded products, M86 Security, the M86 Security logo and M86-branded products are registered trademarks under license by M86 Security. All other product and company names mentioned herein are trademarks or registered trademarks of their respective companies. All rights reserved.

### Trademarks

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

## Contents

<b>1</b>	<b>Introduction</b>	<b>4</b>
1.1	What is the Mobile Security Client?	4
1.2	What is the purpose of this guide?	4
1.3	Administrator Guide Conventions	4
1.4	Terminology	4
<b>2</b>	<b>Client Architecture</b>	<b>5</b>
2.1	Functionality	5
2.2	Components & Outline Operation	5
2.3	Local IP Port Usage	6
2.4	User Identification	6
2.5	On / Off Premise behavior	6
<b>3</b>	<b>Supported Operating System and Browsers</b>	<b>8</b>
<b>4</b>	<b>Installation &amp; Removal</b>	<b>8</b>
4.1	Client Settings at Install	8
4.2	Client Deployment	8
4.3	Microsoft Windows – manual installation/removal	9
4.4	Apple Mac OSX – manual installation/removal	10
4.5	Client Tamper Resistance	11
<b>5</b>	<b>Server Selection</b>	<b>11</b>
5.1	Initial start-up	11
5.2	Auto-tuning	11
5.3	Fail-over	11
<b>6</b>	<b>PAC File</b>	<b>12</b>
6.1	Structure	12
6.2	Enforcement	12
<b>7</b>	<b>Tray Icon Menu Functions</b>	<b>14</b>
7.1	MSC Status	14
7.2	Options	14
7.3	Hiding System Icon Tray (M86 WFR Only)	15
<b>8</b>	<b>Automatic Updates</b>	<b>15</b>
8.1	MSC Configuration Updates	15
8.2	On-going MSC Code Updates	15

## 1 Introduction

### 1.1 What is the Mobile Security Client?

Trustwave (formerly M86) Mobile Security Client (MSC) is used by the Trustwave (formerly M86) Secure Web Gateway and Trustwave (formerly M86) Web Filter to perform Internet traffic scanning / 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<sup>1</sup> to validate end users before granting them Internet access based on their profiles.

### 1.2 What is the purpose of this guide?

This guide is intended to help systems 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 Web Filter (WFR) v 5.0** products. 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**.

### 1.3 Administrator Guide Conventions

The following icons are used throughout this guide:



**NOTE:** The “note” icon is followed by italicized text providing additional information about the current topic.



**TIP:** The “tip” icon is followed by italicized text giving you hints on how to execute a task more efficiently.



**WARNING:** The “warning” icon is followed by italicized text cautioning you about making entries in the application, executing certain processes or procedures, or the outcome of specified actions.



**IMPORTANT:** The “important” icon is followed by italicized text informing you about important information or procedures.

### 1.4 Terminology

The following terms are used throughout this administrator 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.

<sup>1</sup> When used with the Web Filter product, user certificates are optional.

## 2 Client Architecture

### 2.1 Functionality

The Mobile Security Client (MSC) performs the following functions:

- Re-direct web traffic from the worker's PC to a Server component (CloudScanner for SWG, Mobile Server for WFR).
- Select the most appropriate server and deal with fail-over between Servers.
- Secure the communications between the client and the Servers (ensure privacy).
- Identify and authenticate the user and machine using certificates (or login details on WFR).
- Enforce the MSC and web browser configuration (tamper resistance).

### 2.2 Components & Outline Operation

The MSC consists of a number of components installed on the mobile worker 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<sup>2</sup>.
- 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, also to perform activity checks, configuration updates and client code updates.

This client architecture is shown in the diagram below:

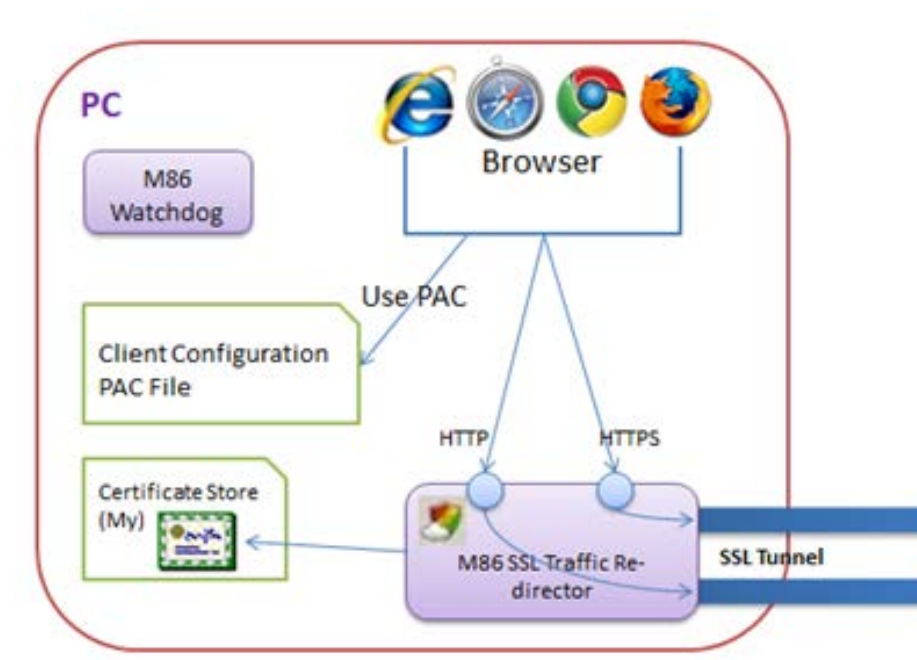


Figure: MSC Architecture.

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.

<sup>2</sup> User certificates are not required when installing the MSC in Simple Client mode in a Web Filter deployment.

## 2.3 Local IP Port Usage

Trustwave SSL traffic redirector is listening to several local ports as described in the following table. Please refer to the MSC Architecture diagram above when referring to the table.



**Note:** All Local Client ports are configurable.

"Local Client" IP Port #	Purpose
27778	Control port used by the Trustwave/M86 Watchdog for configuration and binary updates as well as heartbeat when configured.
HTTP1	Used by the browser to redirect <b>HTTP</b> traffic through a specific Server #1 for scanning purposes. The browser will redirect HTTPS through this port if HTTPS is not configured.
HTTPS1	Used by the browser to redirect <b>HTTPS</b> traffic through a specific Server #1 for scanning purposes.
HTTP2	Used by the browser to redirect <b>HTTP</b> traffic through a specific Server #2 for scanning purposes. The browser will redirect HTTPS through this port if HTTPS is not configured.
HTTPS2	Used by the browser to redirect <b>HTTPS</b> 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 the Simple Client Mode then 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.

### 2.4.2 User Certificates

If user certificates are being 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 M86 SSL traffic redirector 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.

## 2.5 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 an on/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.

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* or the *Trustwave Web Filter User Guide for Mobile Security Client* respectively.

### 3 Supported Operating System and Browsers

M86 Mobile Security Client v2.0.1 Officially Supported O/S Platforms and Browsers				
O/S Platform	Browser types and versions			
	Internet Explorer	Safari	Firefox	Chrome
Windows XP (SP3)	8	n/a	13,14	20,21
Windows Vista (SP1)	8	n/a	13,14	20,21
Windows 7	8,9	n/a	13,14	20,21
Mac OSX Snow Leopard	n/a	5.6	13,14	20,21
Mac OSX Lion	n/a	5,6	13,14	20,21

*\* The Mobile Security Client v2.0.1 will also work with other browsers and programs that can be configured to make use of the Windows Internet connection settings or a Proxy Auto Configuration file . In these cases filtering can be implemented, but browser/application configuration is *\*not\** enforced. **NOTE:** Only the scenarios defined in the table above are officially supported by M86 Security.*

*Updated: August 14, 2012*

## 4 Installation & 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 PAC (Proxy Auto Configuration) file is set. Browsers and other applications that use the system setting 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. This setting of network configuration happens both at MSC install and periodically whilst the MSC is running to help mitigate tampering.

### 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 product the client can be distributed by using the built-in email feature of the SWG Policy Server and then manually installed 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 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 even 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 below.



**NOTE:** 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<sup>3</sup>.

## 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 above 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.

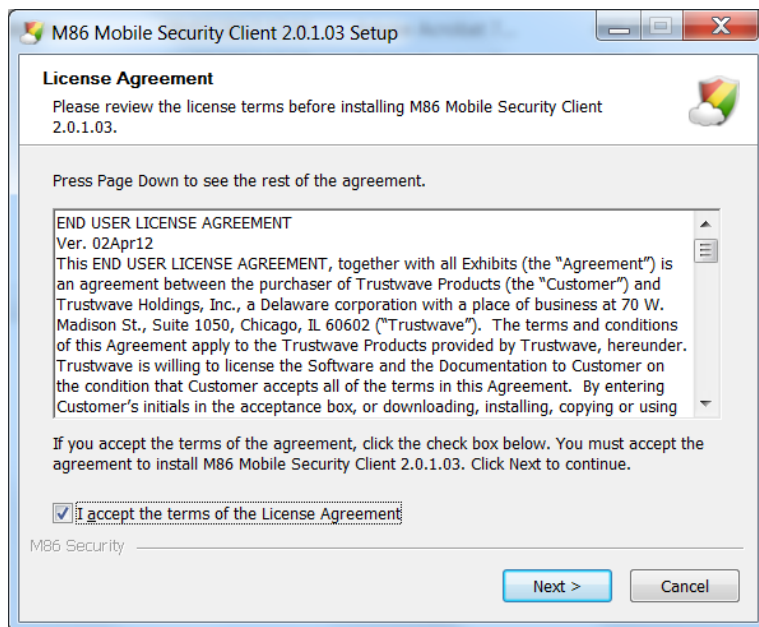
### 4.3.2 Install Procedure for Windows



**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 “/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 is successfully finished.

<sup>3</sup> 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.

### 4.3.3 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 **M86 Mobile Security Client**.
3. Follow the uninstall dialogue.
4. Depending server side settings (SWG: Cloud Configuration Tab – “Enable Client Uninstall Warning”) a customisable 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 above for operating system and browser versions.
- All local ports on the Mac PCs 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)
3. Follow the installer dialogue
4. Accept the License Agreement.
5. Restart the machine once the installation is successfully completed

### 4.4.3 Uninstall procedure for Mac

#### To uninstall the Mac client:

1. Search for M86ClientUninstaller in Spotlight and double-click on it (as an application).
2. Follow the uninstall dialogue.
3. Depending server side settings (SWG: Cloud Configuration Tab – “Enable Client Uninstall Warning”) a customisable Uninstall Warning dialogue box may appear.
4. To continue the uninstall process select **Yes**, or to abort the process select **No**.

## 4.5 Client Tamper Resistance

M86 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:

- o Every 15 seconds the client checks for changes to the Proxy settings on the PC and returns them to the original values.
- o If a user is able to stop the MSC client process, it will automatically re-start again in around 10 seconds.
- o Every hour the PAC file configuration is refreshed using the official copy (see also section 6.2 below).
- o If the user attempts to remove the client through the uninstall process, a customisable warning banner is presented.

## 5 Server Selection

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

### 5.1 Initial start-up

On start-up the MSC uses its default Server whilst 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 whilst 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 times as the test results show its reputation has improved sufficiently that it can be used again.

### 5.3 Fail-over

In addition to auto-tuning, keep-alive tests are performed. If the currently used server becomes unresponsive (unavailable) the MSC will fail-over 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 M86 SSL Traffic Re-director as its proxy and by this redirects Web traffic to the server.

### 6.1 Structure

The MSC PAC file operates under several conditions, all aiming 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 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. Needed, for example, to negotiate WiFi billing systems in Airports and Hotels.

## 6.2 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 behaviour 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.

If the administrator chooses the MSC to not enforce the PAC file, he/she must make sure that the PAC file in use has the correct proxy definitions; otherwise the traffic won't be redirected through the local M86 SSL Traffic Re-director process.

## 7 Tray Icon Menu Functions

### 7.1 MSC Status

The tray icon notifies the user about the MSC status. Possible states are:



Enabled – normal operation.



Disabled



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

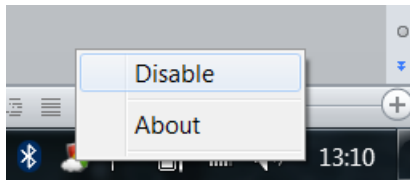



Error condition

### 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 (M86 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 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, 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<sup>4</sup> 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.



70 West Madison St. tel 312.873.7500  
Suite 1050 fax 312.443.8028  
Chicago, IL 60602 www.trustwave.com

<sup>4</sup> Applies to M86 SWG version 10.2 and M86 MSC v2.0.1 onward.