



M86 Web Filter

# USER GUIDE

for M86 Mobile Security Client

Software Version: 5.0.00  
Document Version: 02.01.12

# **M86 WEB FILTER USER GUIDE FOR M86 MOBILE SECURITY CLIENT**

© 2012 M86 Security  
All rights reserved.

Version 1.01, published February 2012 for Web Filter software  
release 5.0.00

Printed in the United States of America

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form without prior written consent from M86 Security.

Every effort has been made to ensure the accuracy of this document. However, M86 Security makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. M86 Security shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. Due to future enhancements and modifications of this product, the information described in this documentation is subject to change without notice.

## **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.

Part# WF-MSC-UG\_v1.01-1202

---

# CONTENTS

<b>INTRODUCTION .....</b>	<b>1</b>
<b>M86 Mobile Security Client .....</b>	<b>1</b>
<b>About this User Guide .....</b>	<b>2</b>
<b>Environment Requirements .....</b>	<b>3</b>
Workstation Requirements .....	3
Network Requirements .....	4
Synchronization .....	5
Remote Filtering Components .....	5
Reporting Options .....	5
<b>Network Server, Client Communications .....</b>	<b>6</b>
Types of Certificates Used .....	7
PAC File Configuration, Deployment .....	8
<b>Work Flow Overview .....</b>	<b>9</b>
Internal Mode Server Flow .....	9
Enterprise PKI Mode Server Flow .....	10
Client Request Flow to the Mobile Filter .....	11
Client Request Flow to On/Off Site Filters .....	12
<b>CONFIGURATION .....</b>	<b>14</b>
<b>Preliminary Setup .....</b>	<b>14</b>
<b>Set the Mobile Operation Mode .....</b>	<b>15</b>
<b>Configure Mobile Server, Client Settings .....</b>	<b>16</b>
Generate Certificates, Retrieve CRL .....	17
Step 1: Set Certificate Management Mode .....	18
Step 2: Download, Import the CA Certificate .....	18
Step 3: Generate, Sign the Server Certificate .....	21
Step 4: Import the Server Certificate .....	23
Step 4A: Import a CSR-based Certificate .....	23
Step 4B: Import a Server Certificate .....	25
Retrieve the CRL File .....	27

- Test CRL Location ..... 27
- Retrieve CRL On Demand ..... 28
- Schedule CRL Retrieval ..... 28
- Configure the Client ..... 29
  - Specify Connection Settings ..... 30
  - Specify Client Options ..... 32
  - Specify IPs and URLs to be Bypassed ..... 34
  - Download the Client Installer or PAC File ..... 36
    - Download the Client Installer ..... 36
    - PAC File ..... 36
- TROUBLESHOOT FILTERING ..... 37**
  - Set the Troubleshooting Mode ..... 37**
- APPENDICES ..... 39**
  - Appendix A ..... 39**
    - Performance Statistics ..... 39
  - Appendix B ..... 40**
    - Glossary ..... 40
- INDEX ..... 41**

# INTRODUCTION

## **M86 Mobile Security Client**

M86 Mobile Security Client (MSC) performs Internet filtering and blocking on mobile workstations physically located outside your organization. This product uses a Web Filter configured in the mobile mode, certificates for authentication purposes, and the MSC client installed on each mobile workstation.

MSC ensures Internet activity of all end users located outside the organization will be tracked and filtered in the same manner as end users located on the premises, thereby giving you, the administrator, assurance that your organization will be protected against lost productivity, network bandwidth issues, Internet security threats, and possible legal problems that can result from the misuse of Internet resources on an unfiltered, remote, workstation.

## About this User Guide

This user guide addresses the network administrator designated to configure and manage the mobile Web Filter server on the network. The manual is organized into the following sections:

- **Introduction** - Overview of this product and how it functions in the environment.
- **Configuration** - How to configure the Web Filter user interface for Mobile Security Client usage.
- **Troubleshoot Filtering** - How to troubleshoot mobile server filtering.
- **Appendices** - Appendix A features a chart containing Performance Statistics. Appendix B provides a Glossary of technical terminology used in this user guide.
- **Index** - Subjects and the first page numbers where they appear in this user guide.

# Environment Requirements

The following requirements must be met in the environment in order to use MSC:

## ***Workstation Requirements***

System requirements for the administrator's workstation include the following:

- Windows XP, Vista, or 7 operating system running:
  - Internet Explorer (IE) 8.0
  - Firefox 6.0
  - Google Chrome 13.0
  - Safari 5.0
- Macintosh OS X Version 10.6 or 10.7 running:
  - Safari 5.0
  - Firefox 6.0
  - Google Chrome 13.0
- Session cookies from the Web Filter must be allowed in order for the Administrator console to function properly
- Pop-up blocking software, if installed, must be disabled
- JavaScript enabled
- Java Virtual Machine
- Java Plug-in (use the version specified for the Web Filter software version)

## Network Requirements

Network requirements to use MSC include the following:

- Web Filter with Mobile mode enabled, either:
  - Web Filter Appliance - 32-bit platform models: 70, 71, 80, 84, 85; 64-bit platform models 300, 500, 700  
or
  - Web Filter Virtual - Web Filter image downloaded to your appliance running in an environment that supports Virtualization Technology



**NOTES:** *WFR (models 350 and 550) and IR Web Filter (model 81) appliances cannot be used as mobile servers.*

*See the Appendix A for a chart containing performance statistics on each appliance type running MSC.*

- Server designated for generating and issuing certificates, either:
  - the mobile Web Filter (if using the internal certification mode)  
or
  - a server on the network (such as LDAP) that can communicate with the mobile Web Filter and mobile workstations via an external Public Key Infrastructure (if using the Enterprise PKI certification mode)



**NOTE:** *In this release, only the external PKI mode is available.*

- High speed connection from the mobile Web Filter to mobile PCs and pertinent devices on the network, such as an LDAP server, if applicable



**NOTE:** *Multiple mobile Web Filters can be set up for use in a failover situation.*



## Synchronization

In a synchronization environment, mobile settings are not synchronized.

For environments with a WFR (models 350 and 550) or an IR (model 81), in order to use the synchronization feature, M86 recommends using a Virtual Web Filter, since a WFR or IR cannot be used as a source or target server, nor configured to be used as a mobile server.

## Remote Filtering Components

Remote filtering components for using MSC include:

- Web Filter configured to use the Mobile mode for filtering mobile workstations



**NOTE:** Multiple mobile Web Filters can be set up for use in a failover situation.

- MSC client software installed on each end user's mobile workstation



**NOTE:** In order for mobile end user traffic to be logged under a specific username, a domain profile or group profile must be set up on the mobile Web Filter. Without either of these profiles established, mobile end user traffic will be logged under the "IPGROUP" or "DEFAULT" (Global Group) profile.

## Reporting Options

As with the standalone Web Filter on the intranet, end user Internet traffic captured by the mobile Web Filter can be submitted to the local M86 Security Reporter (SR) or M86 Enterprise Reporter (ER) for processing.

Using the SR Report Manager or ER Web Client, in minutes an administrator can generate customized reports showing the remote end user's online activity.

## **Network Server, Client Communications**

MSC mobile filtering requires the authentication of end user credentials—via a validation of certificates on the mobile workstation and mobile Web Filter—in order for the user’s filtering profile to be obtained for his/her Internet usage.

Prior to enabling the MSC feature, the administrator determines whether to solely use the mobile Web Filter to communicate with mobile workstations located off premises in the certificate issuance and validation process, or to use a network device (e.g. LDAP server) along with the mobile Web Filter to communicate with mobile workstations.

Use of the mobile Web Filter without an external device requires the internal mode configuration setup, in which the Web Filter signs and issues certificates to mobile workstations.

Use of an external server with the mobile Web Filter requires the Enterprise PKI mode setup, in which the designated external device signs and issues certificates to the mobile Web Filter and mobile workstations.

## Types of Certificates Used

The certificate issuance and validation process utilizes the following types of certificates:

- **Certification Authority (CA)** - This certificate is generated and signed by the device authorized to issue digital certificates to the mobile Web Filter and mobile workstations. In the internal mode, the CA certificate would be signed by the mobile Web Filter and issued to itself and mobile workstations.

If a root CA certificate and intermediate CA certificate are used for signing certificates, both of these CA certificates must be imported into the mobile Web Filter.

- **Server certificate** - This certificate validates the mobile Web Filter's internal SSL traffic redirector component that communicates with MSC clients. The server certificate is generated on the mobile Web Filter and signed by the device authorized to issue certificates to the mobile Web Filter. This certificate is used along with the CA certificate(s) in the validation process between the mobile Web Filter and mobile workstations.



**NOTE:** A signed server certificate can be uploaded to the mobile Web Filter along with the private key .pem (privacy enhanced mail) file and password.

- **User certificate** - This certificate validates the end user on his/her workstation. The user certificate is generated by the device authorized to issue certificates to the mobile Web Filter and mobile workstations.

## ***PAC File Configuration, Deployment***

The Proxy Auto-Configuration (PAC) file configured on the mobile Web Filter is the client component that communicates with the end user's browser and the component that redirects SSL traffic. The configured PAC file is packaged in the client installer file, ready to be downloaded and deployed to mobile workstations. When installed on end user mobile workstations, the client checks for new configuration updates every 60 minutes.

The configured PAC file is also available for downloading as a standalone file for review and customization prior to deployment to mobile workstations.



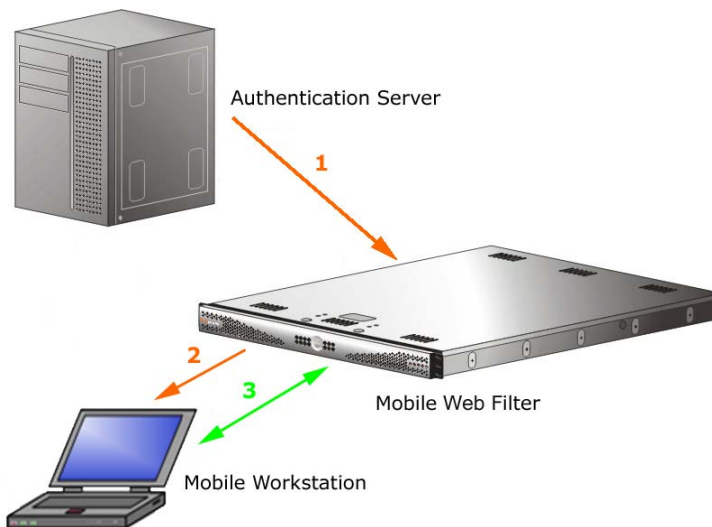
***NOTE:*** *If the PAC file is customized, the PAC file packaged inside the client will not be used. In this scenario, provisions must be made for the customized PAC file to perform the same functions executed by the PAC file packaged inside the client. Additionally, a customized PAC file will not be automatically updated by the mobile Web Filter.*

# Work Flow Overview

## *Internal Mode Server Flow*

In the internal mode, the following occurs in the environment:

1. The authentication server gives the mobile Web Filter the group and user profiles.
2. The mobile Web Filter generates certificates for itself and end user mobile workstations, and issues these certificates to mobile workstations.
3. When a request is made from a mobile workstation off the organization's premises, certificates between that workstation and the mobile Web Filter are verified before the request is handled by the client, and then processed by the mobile Web Filter.



*Fig. 2-1 Internal mode server flow*

## Enterprise PKI Mode Server Flow

In the Enterprise PKI mode, the following occurs in an environment with an authentication server designated to sign certificates:

1. The authentication server that stores group and user profiles generates and signs certificates that are imported into the mobile Web Filter.
2. The authentication server generates and signs certificates that are issued to end user mobile workstations.
3. When a request is made from a mobile workstation off the organization's premises, certificates between that workstation and the mobile Web Filter are verified before the request is handled by the client, and then processed by the mobile Web Filter.



Fig. 2-2 Enterprise PKI mode server flow

## Client Request Flow to the Mobile Filter

With the client installed on a mobile workstation located outside of the organization, the following events occur on the workstation when the end user makes a URL request:

1. The browser consults the PAC file to determine which port to use for submitting the URL request to the SSL traffic redirector component.
2. The HTTP/HTTPS request is submitted to the SSL traffic redirector.
3. Certificates stored on the workstation are used for validating communications between the workstation, mobile Web Filter, SSL traffic redirector, and certificate authority.
4. The request is submitted to the mobile Web Filter.
5. The mobile Web Filter determines if the request should pass to the Internet, based on the end user's profile.

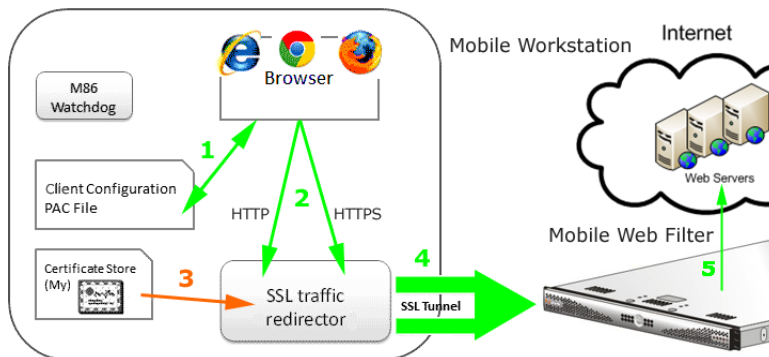


Fig. 2-3 Mobile workstation flow to mobile Web Filter (internal PAC file)



**NOTE:** M86 Watchdog is a service in the client that builds and updates configuration files, performs keep alive checks, and enforces IE, Firefox, and Google browser types. Every two minutes the client informs the mobile Web Filter who is logged in on the mobile workstation.

## Client Request Flow to On/Off Site Filters

When the end user submits a URL request, the client determines whether the mobile workstation is presently located on or off the organization’s premises, based on whether or not it is able to communicate with the Web Filter on the premises.

If the client cannot reach the intranet Web Filter, the following scenario occurs:

1. The client submits the URL request to the mobile Web Filter in the DMZ.
2. The mobile Web Filter checks the end user’s filtering profile to see whether the end user should access the requested content, or receive a warning or block page instead.
3. If the URL request is allowed, the mobile Web Filter passes the request to the Internet. If the request is disallowed, the appropriate response is returned to the workstation.

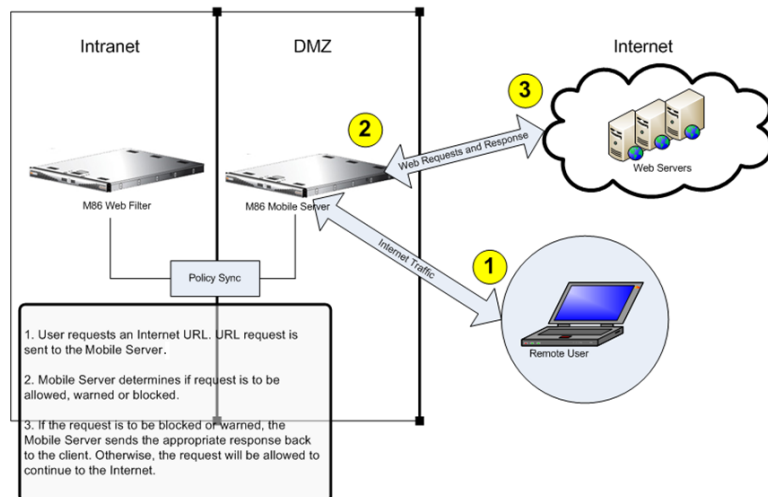


Fig. 2-4 Web Filters on and off premises, and workstation URL request



4. If the end user comes into the organization, logs into his/her workstation and is authenticated on the internal network, the client detects that the workstation is now located on the premises, and the end user is then filtered by the Web Filter on the intranet, and not by the mobile Web Filter.

# CONFIGURATION

This portion of this user guide contains information on how to configure the mobile Web Filter user interface to generate and/or use certificates for devices employed in the authentication process, and to prepare the client for deployment to end user mobile workstations.

## Preliminary Setup

Basic requirements for preliminary network setup are as follows:

- Port 81 must be open on the network for block page requests.
- At your option, set up the mobile Web Filter in the WAN network's DMZ for extra security purposes.
- In the Enterprise PKI mode, a dedicated external device (e.g. LDAP server) must be established for generating, issuing, and storing certificates.

## Set the Mobile Operation Mode

The Operation Mode window is used for setting the Web Filter to use the mobile mode for filtering mobile workstations.

1. Navigate to System > Mode > Operation Mode.
2. In the Mode frame, choose “Mobile”:



Fig. 3-1 Operation Mode window, Mobile mode

3. Click **Apply** to set the mobile mode and to display the Mobile menu topic in the System tree. This menu includes the Certificate Management and Configuration sub-topics.



**NOTE:** Enabling the mobile mode feature disables Policy > Global Group > Range to Detect since a mobile Web Filter does not use this feature to identify and filter end users.

## Configure Mobile Server, Client Settings

MSC is set up on this Web Filter by using the Certificate Management and Configuration windows, accessible from the Mobile menu.

The first step in setting up MSC is to use the Certificate Management wizard to generate and import certificates into this Web Filter. After completing all steps in the wizard, verify that a list of active and revoked end user certificates can be obtained from the location where these certificates are stored.

The second step in setting up MSC is to use the Configuration wizard to create the Proxy Auto-Configuration (PAC) file which tells the client how to communicate with pertinent devices on the network. The PAC file can then be downloaded for review and modification, or packaged in the client within the installer file for ready deployment to end user mobile workstations.

## Generate Certificates, Retrieve CRL

Navigate to System > Mobile > Certificate Management to display the Certificate Management window:

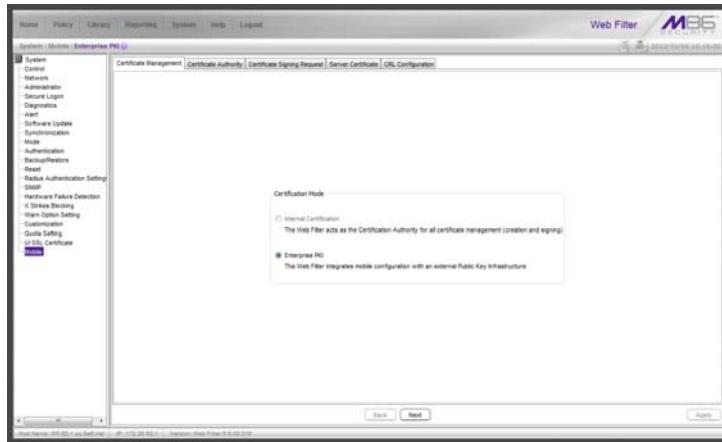


Fig. 3-2 Certificate Management window, Enterprise PKI option

Use tabs in the Certificate Management wizard to set up certificate criteria for MSC.




**NOTE:** At any point in the wizard, settings can be saved by clicking **Apply**.



**TIP:** On a Windows machine, downloaded certificates are named *certnew.cer* by default. Since you will be downloading two different signed certificates to be installed on the mobile Web Filter, M86 recommends renaming each certificate—immediately after it is downloaded—for its associated usage. For example, the CA certificate might be renamed "ca.cer" and the SSL traffic redirector server certificate you download next might be renamed "server.cer".

## Step 1: Set Certificate Management Mode

The Certificate Management tab includes Certification Mode options for using the Mobile Security Client: Internal Certification and Enterprise PKI.

 **NOTE:** “Internal Certification” is disabled since this release only supports the Enterprise PKI mode.

Click **Next** to go to the Certificate Authority tab.

## Step 2: Download, Import the CA Certificate

The Certificate Authority tab is used for uploading the Certificate Authority certificate of the device to be used for generating and issuing certificates.

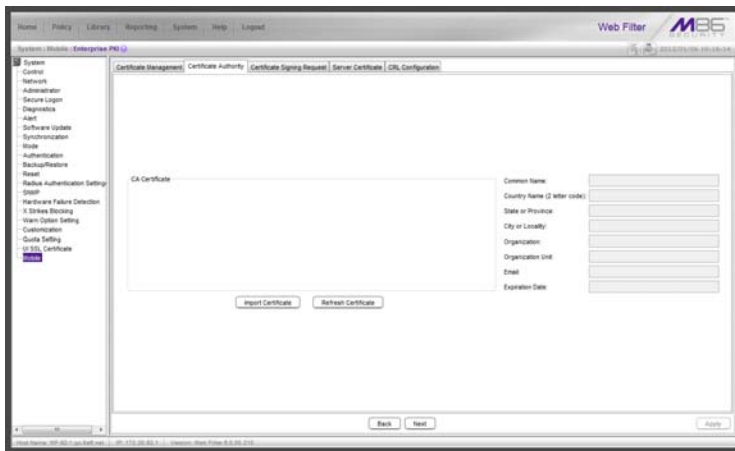


Fig. 3-3 Certificate Authority tab

1. Click **Import Certificate** to open a new window/tab for importing the CA certificate that was generated on the server designated to sign certificates:



Fig. 3-4 CA Certificate window

2. Under Root CA Certificate, click **Browse...** to search for the downloaded root CA certificate. If this is the only CA certificate that needs to be uploaded, proceed to step 4.
3. Under Intermediate CA Certificate, click **Browse...** to search for the downloaded intermediate certificate.
4. Click **Import CA Certificate** to upload the certificate(s) to this mobile Web Filter.
5. After receiving confirmation of successful CA certificate importation, return to the Certificate Authority tab and click **Refresh Certificate** to display the certificate contents in the CA Certificate box above, and server information in the fields to the right:

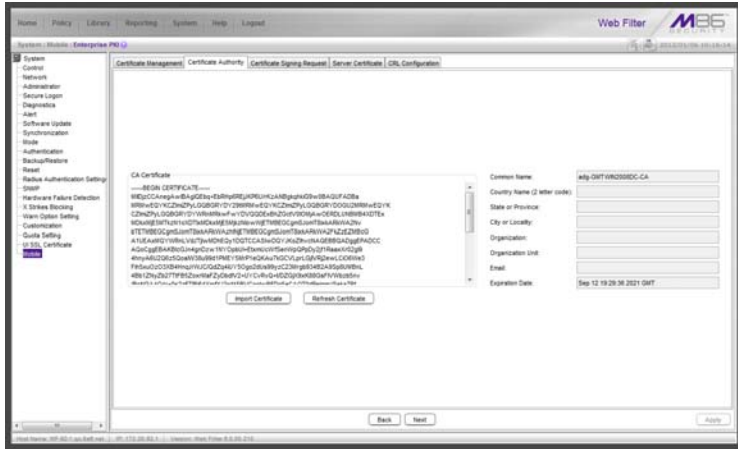


Fig. 3-5 Refreshed CA Certificate

6. Click **Next** to go to the Certificate Signing Request tab to generate the server certificate.

If the server certificate was generated without using the Certificate Signing Request tab, or was already generated and signed in a prior session using this tab, advance to Step 4: Import the Server Certificate for instructions on using the Server Certificate tab to import the signed server certificate into this mobile Web Filter along with the .pem private key file and password.



## Step 3: Generate, Sign the Server Certificate

The Certificate Signing Request tab is used for generating the SSL traffic redirector component server certificate that the client will use for communicating with this mobile Web Filter.

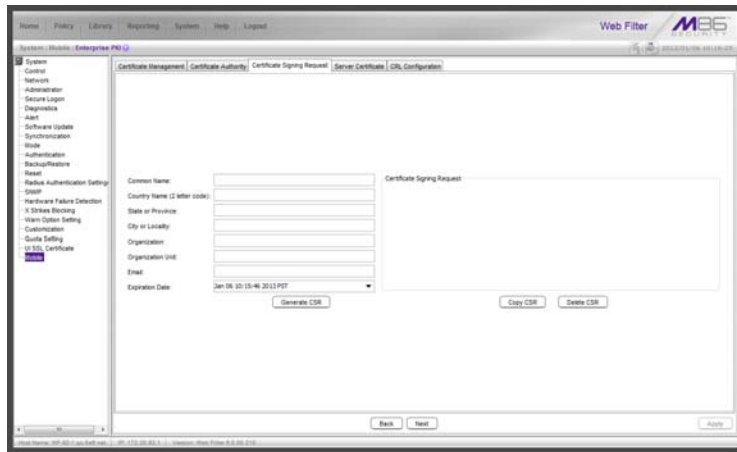


Fig. 3-6 Certificate Signing Request tab

1. Make entries in these fields:
  - a. **Common Name:** Full DNS hostname of this server, as entered in Network > LAN Settings > Host Name field, such as **logo.server.com**.
  - b. **Country Name (2 letter code):** Two-character country code, such as **US**.
  - c. **State or Province:** Full name or code identifying your state or province, such as **CA** or **California**.
  - d. **City or Locality:** Name of your organization's city or principality, such as **Irvine**.
  - e. **Organization:** Name of your organization, such as **Logo Corporation**.
  - f. **Organization Unit:** Name of your department, such as **Administration**.

- g. **Email:** Your email address.
- 2. The **Expiration Date** field displays the date and time a year from the moment this window was last refreshed, using the following format: abbreviated name of this month, number of the day within this month, time (HH:MM:SS), coming year (YYYY), and time zone code.

The date can be changed by clicking the down arrow at the far right of this field to open the calendar, navigating to the selected date, and then double-clicking it to close the calendar and populate this field with the new date.

- 3. Click **Generate CSR** to generate the server certificate. The successfully generated certificate populates the Certificate Signing Request box to the right with the contents of the certificate:

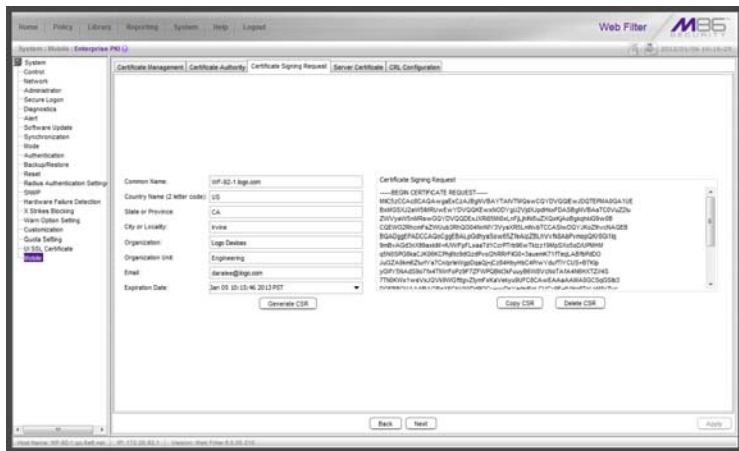



Fig. 3-7 Generated Certificate Signing Request

 **NOTE:** Click **Delete CSR** if any criteria previously specified in this tab has changed and you need to generate a new certificate.

- 4. Click **Copy CSR** to copy the contents of the server certificate to the clipboard. These contents need to be pasted in the external server’s certificate request page so that the server certificate can be signed.

5. After the signed server certificate is downloaded to your workstation, click **Next** to go to the Server Certificate tab.

## Step 4: Import the Server Certificate

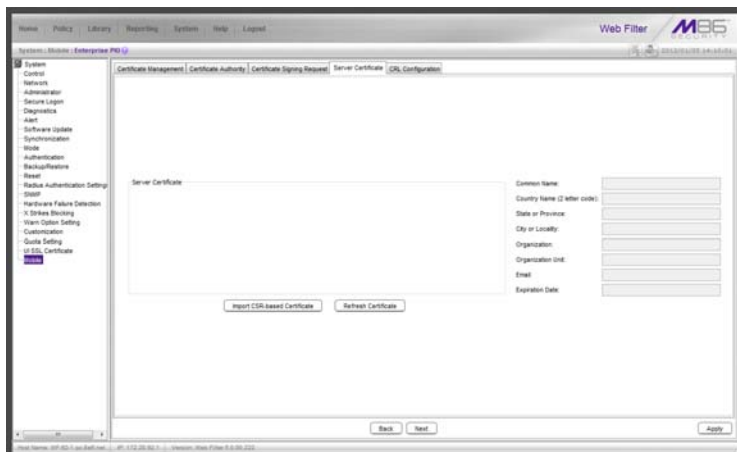
The Server Certificate tab is used for importing the server certificate into this mobile Web Filter. The import button and import process differs depending on whether or not the server certificate was generated during this session by using the Certificate Signing Request tab.

If the server certificate was generated in this session using the Certificate Signing Request tab and has been signed, proceed to Step 4A: Import a CSR-based Certificate.

If the server certificate was previously generated and signed, and is ready to be imported with a serverkey.pem file and .PEM password, proceed to Step 4B: Import a Server Certificate.

### Step 4A: Import a CSR-based Certificate

1. Go to the Server Certificate tab:



*Fig. 3-8 Server Certificate tab for importing CSR-based certificate*

Click **Import CSR-based Certificate** to open the CSR-based Server Certificate window/tab:



*Fig. 3-9 CSR Certificate window*

2. Click **Browse...** to search for the signed server certificate.
3. When the certificate is found, click **Import CSR-based Certificate** to import that certificate into this mobile Web Filter.
4. Return to the Server Certificate tab and click **Refresh Certificate** to display the certificate contents in the Server Certificate box above, and server information in the gray fields to the right:

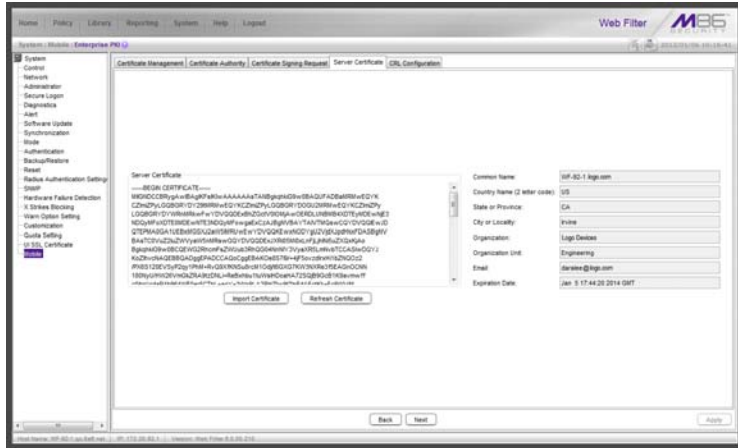


Fig. 3-10 Signed server certificate imported

5. Click **Next** to go to the CRL Configuration tab.

## Step 4B: Import a Server Certificate

1. Go to the Server Certificate tab:

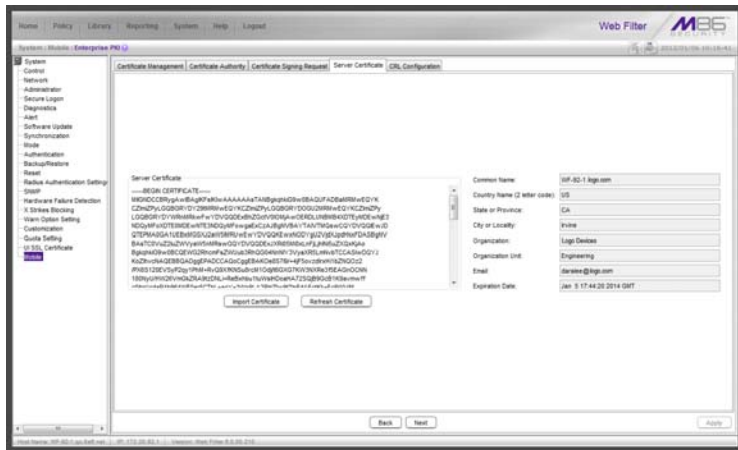


Fig. 3-11 Server Certificate tab for importing non-CSR certificate

Click **Import Certificate** to open the Server Certificate window/tab:



*Fig. 3-12 Server Certificate window*

2. At the **Certificate** field, click **Browse...** to search for the signed server certificate.
3. At the **Private Key** field, click **Browse...** to search for the serverkey.pem file.
4. Enter the .PEM **Password**.
5. Click **Import Certificate/Private Key** to import the certificate, and .PEM file and password into this mobile Web Filter.
6. Click **Next** to go to the CRL Configuration tab.

## Retrieve the CRL File

The CRL Configuration tab is used for retrieving the Certification Revocation List file stored on the device that issues and stores certificates. The path where the CRL is stored can be tested for verification of file retrieval; a schedule can be set for retrieving the file; and the file can be retrieved on demand.

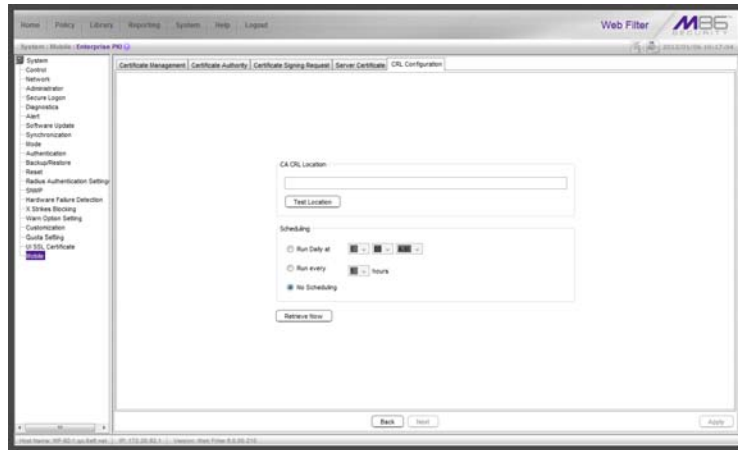


Fig. 3-13 CRL Configuration tab

## Test CRL Location

1. In the CA CRL Location frame, type in the URL of the server where certificates are stored.
2. Click **Test Location** to verify that the server can be accessed from this mobile Web Filter.

## Retrieve CRL On Demand

To download the CRL now:

1. In the CA CRL Location frame, enter the URL of the certificate storage server.
2. Click **Apply** to save the location.
3. Click **Retrieve Now**.



**NOTE:** Clicking **Retrieve Now** restarts the SSL traffic redirector component, and any end users logged into their mobile workstations running the MSC client will momentarily lose their Internet connections. Such an action may in particular affect end users taking online tests or submitting online forms.

## Schedule CRL Retrieval

1. In the Scheduling frame, set the schedule for retrieving the CRL from the server where certificates are stored by choosing one of three options:
  - **Run Daily at** - If choosing this option, specify the hour (1 - 12), minutes (1 - 59), and "A.M." or "P.M."
  - **Run every** - If choosing this option, specify the hours (1 - 12) between intervals from the moment **Retrieve Now** is clicked.
  - **No Scheduling** - If using this default option, you can click **Retrieve Now** at any time to download the CRL on demand.
2. Click **Apply** to save your settings.



## Configure the Client

Navigate to System > Mobile > Configuration to display the Configuration window:

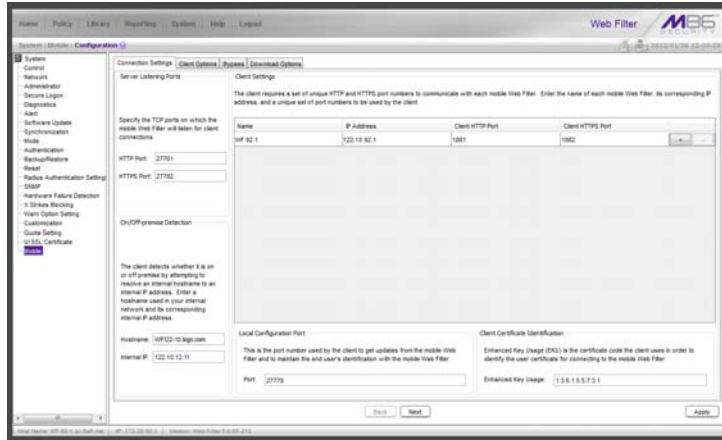


Fig. 3-14 Certificate Management window, Enterprise PKI option

Use tabs in the Configuration wizard to create the MSC client. The completed client can be downloaded within the installer file for ready deployment, or its Proxy Auto-Configuration (PAC) file can be downloaded for review and modification before deployment to end user workstations.



**NOTE:** At any point in the wizard, settings can be saved by clicking **Apply**.

## Specify Connection Settings

---

The Connection Settings tab is used for specifying ports the client will use to communicate with pertinent devices on the network, and for entering the server certificate EKU so the client will recognize the mobile server.

1. In the Server Listening Ports frame, enter the **HTTP Port** this mobile Web Filter will use when listening for connections from the client. The default is *27781*.
2. Enter the **HTTPS Port** this mobile Web Filter will use when listening for connections from the client. The default is *27782*.
3. In the On/Off-premise Detection frame, enter the **Host-name** of a device on the internal network, and its corresponding **Internal IP** address. The client will use this criteria to determine whether the mobile workstation is currently on site or off site.
4. The Client Settings frame includes a table for specifying mobile Web Filters, the Local Configuration Port frame, and the Client Certificate Identification frame.

In the table, enter the following information for each mobile Web Filter to be used:

- a. **Name** of the mobile Web Filter.
- b. **IP Address** of the mobile Web Filter.
- c. Unique **Client HTTP Port** number to be used by mobile workstations to send traffic to the mobile Web Filter.
- d. Unique **Client HTTPS Port** number to be used by mobile workstations to send traffic to the mobile Web Filter.



**TIP:** Click the “+” at the end of the row to add another row in the table. Click the “-” at the end of the row to remove the current row from the table.

5. In the Local Configuration Port frame, by default the **Port** number is 27778. This port number, which can be modified, is used by the SSL traffic redirector to check for client configuration updates, and to communicate with the mobile Web Filter that the client should still be connected to that server.
6. In the Client Certificate Identification frame, enter the **Enhanced Key Usage** number from the end user's certificate. The MSC client uses the EKU code to identify the user certificate to use for connecting to the mobile Web Filter.
7. Click **Next** to go to the Client Options tab.

## Specify Client Options

The Client Options tab is used for indicating which optional features will be included in the client.

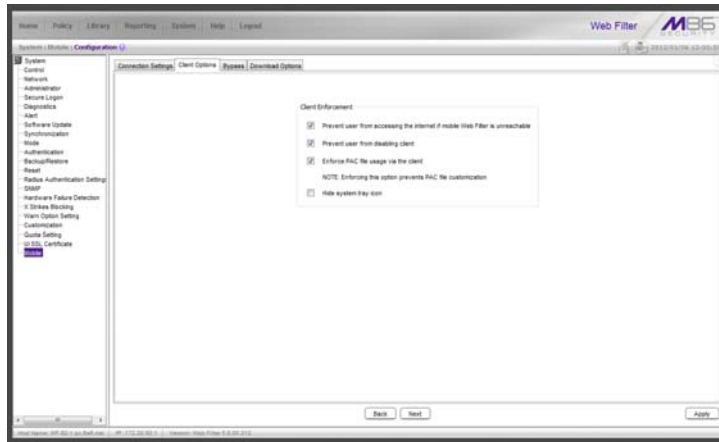


Fig. 3-15 Client Options tab

1. In the Client Options tab, indicate whether to include the following options:
  - a. **Prevent user from accessing the internet if mobile Web Filter is unreachable:** By default this option is enabled, indicating the end user will not be able to access the Internet if the client cannot communicate with the mobile Web Filter.
  - b. **Prevent user from disabling client:** By default this option is enabled, indicating the end user will not be able to disable the client from running on the mobile workstation. If a particular service needs to run that the client is blocking the administrator will need to disable the client to run that service on the workstation.

- c. **Enforce PAC file usage via the client:** By default this option is enabled, indicating settings saved in these tabs will be used by the PAC file on mobile workstations. If the PAC file is downloaded and modified, it will not be used by mobile workstations.
  - d. **Hide system tray icon:** Enabling this option will hide the client icon from displaying in the mobile workstation task bar.
2. Click **Next** to go to the Bypass tab.

## Specify IPs and URLs to be Bypassed

The Bypass tab is used for specifying which domains the client should ignore, and which URLs should be whitelisted.

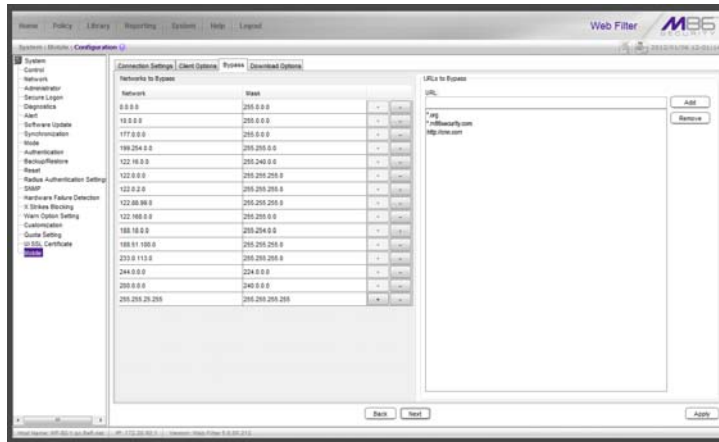



Fig. 3-16 *Bypass tab*

1. By default, the Networks to Bypass table includes rows of Network IP addresses the client should bypass when filtering, and for each domain, its corresponding net Mask. Any of these networks can be removed, but the table must include at least one network.

To add a row to this table, click the “+” at the end of the row, and enter the **Network** IP address and its net **Mask**.

 **TIP:** Click the “-” at the end of an added row to remove that row from the table.

2. In the URLs to Bypass frame, enter a URL to be whitelisted for the client and then click **Add** to include that URL in the list box.

Wildcards can be used in this entry. For example:

- \*.usatoday.com, or top level domain entries such as \*.au, \*.edu, or \*.gov



**TIP:** *To remove a URL from the list box, select the URL and then click **Delete**.*

3. After all settings are made, click **Apply** to create the client installer and PAC file.
4. Click Next to go to the Download Options tab.

## Download the Client Installer or PAC File

The Download Options tab is used for either downloading the client installer or the PAC file.

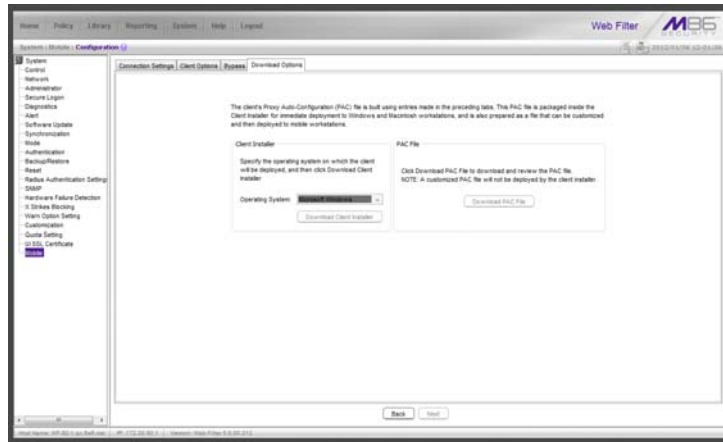


Fig. 3-17 Download Options tab

### Download the Client Installer

1. In the Client Installer frame, select the type of **Operating System** (“Microsoft Windows” or “Mac OS X”) on which the client will be deployed.
2. Click **Download Client Installer** to download that file to your workstation.

### PAC File

In the PAC File frame, click **Download PAC File** if you wish to download the PAC file for review and/or customization prior to deployment to mobile workstations.



**NOTE:** A customized PAC file can only be deployed outside of the client. If using a customized PAC file, any settings made in the PAC file inside the client will not be used by the client. Additionally, any client updates will not be automatically deployed to mobile workstations via the mobile Web Filter.



# TROUBLESHOOT FILTERING

This portion of the user guide provides information on how to access and set the mode in the Web Filter to troubleshoot mobile server filtering.

## Set the Troubleshooting Mode

The Troubleshooting Mode window is used for setting the mobile Web Filter to use the troubleshooting mode to analyze and/or verify mobile workstation filtering by this server.

1. Navigate to System > Diagnostics > Troubleshooting Mode:

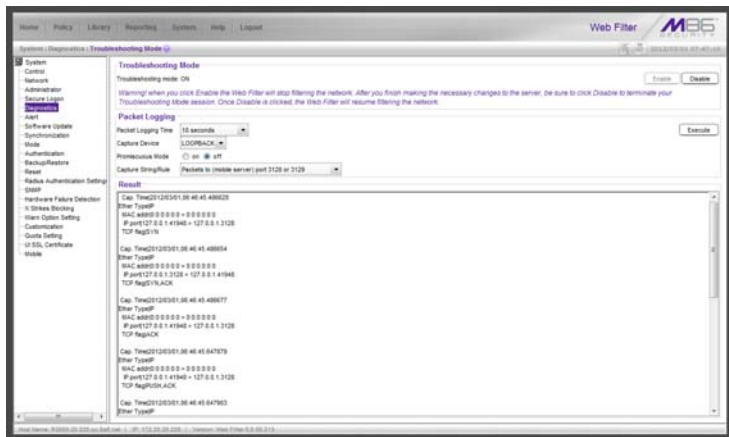


Fig. 4-1 Troubleshooting Mode window

2. Specify the **Packet Logging Time** by making a selection from the pull-down menu for one of the following choices: “10 seconds”, “30 seconds”, “60 seconds”.

By default, this Web Filter set in the mobile mode displays “LOOPBACK” as the **Capture Device**.

3. Click **Enable** to set the troubleshooting mode and to disable filtering.
4. From the **Capture String/Rule** pull-down menu, choose “Packets to (mobile server) port 3128 or 3129”.
5. Click **Execute** to display results in the Result frame.

# APPENDICES

## Appendix A

### *Performance Statistics*

The chart below provides statistics for each supported appliance type running MSC:

<b>Appliance models (mobile servers)</b>	<b>Maximum Users</b>	<b>Maximum hits/sec.</b>
<b>MSA</b> (32-bit model 80)	1,000	75
<b>SL</b> (32-bit models 70 with SSL card, and 84)	2,000	150
<b>HL</b> (32-bit models 71 with SSL card, and 85)	3,000	250
<b>300</b> (64-bit model)	1,000	75
<b>500</b> (64-bit model, SSL card)	2,000	150
<b>700</b> (64-bit model, SSL card)	3,000	250

# Appendix B

## *Glossary*

**Certification Revocation List (CRL)** - A list of valid and revoked user certificates housed on the server that stores these certificates.

**Enhanced Key Usage (EKU)** - In the Enterprise PKI mode, this code identifies the user certificate the MSC client should use for mobile filtering.

**Enterprise PKI** - One of two options available for the mobile mode, this setting indicates the mobile Web Filter will use an external server for storing certificates used in the authentication process.

**Internal Mode** - One of two options available for the mobile mode, this setting indicates the mobile Web Filter will store all certificates used in the authentication process.

**Local Configuration Port** - Used by the SSL traffic redirector to check for client configuration updates and to communicate with the mobile Web Filter that the client connection should be kept alive.

**M86 Watchdog** - A service running in the client that builds and updates configuration files, performs keep alive checks, and enforces IE, Firefox, and Google browser types.

**Proxy Auto-Configuration (PAC)** - This file configured on the mobile Web Filter is the component in the client that communicates with the end user's browser and the component that redirects SSL traffic.

---

# INDEX

## A

administrator workstation requirements 3

## C

certificates, types 7

Certification Authority 7

Certification Revocation List 27

Certification Revocation List (CRL), definition 40

## D

DMZ 12, 14

## E

Enhanced Key Usage (EKU), definition 40

Enterprise PKI, definition 40

environment requirements 3

## F

Firefox 3

## G

Google Chrome 3

## I

Internal Mode, definition 40

Internet Explorer 3

## J

Java Plug-in 3

Java Virtual Machine 3

JavaScript 3

## **L**

Local Configuration Port, definition 40

## **M**

M86 Watchdog, definition 40

Macintosh 3

## **N**

network requirements 4

## **O**

Operation Mode window

mobile mode 15

## **P**

Proxy Auto-Configuration (PAC), definition 40

## **R**

remote filtering components 5

reporting options 5

## **S**

Safari 3

server certificate 7

synchronization 5

system requirements 3

## **U**

user certificate 7

## **W**

Windows 7 3

Windows Vista 3

Windows XP 3