M86 Web Filter

USER GUIDE

for M86 Mobile Security Client

M86 WEB FILTER USER GUIDE
FOR M86 MOBILE SECURITY CLIENT

CONTENTS

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 desig-nated 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 func-tions in the environment.

- **Preliminary Setup** - How to set this server to operate as a mobile Web Filter and specify whether certificates will be generated and stored on this server or another device.

- **Internal Certificate Management** - How to create the MSC client and configure the mobile Web Filter to issue, store, and manage server and user certificates.

- **Enterprise PKI** - How to create the MSC client and configure the mobile Web Filter to communicate with the external device designated to issue, store, and manage server and user certificates.

- **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

To use MSC, the following minimal network requirements must be met:

- 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 Synchronization in this chapter for information on using MSC in a synchronization environment with a Web Filter, WFR, and/or IR.*
- *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)

- 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

If using MSC in a synchronization environment:

- All settings and libraries are synchronized.

- Only the source server—WF, R3000, IR, or WFR—features Mobile and Certificate Management menus.

- An IR or WFR can function as a source or target server, but cannot be used as a mobile server.

The chart below explains which features in the user interface are available on source and target servers if using MSC in a synchronization environment:

WF, R3000, IR or WFR source server:	All MSC-related menus are available, but an IR or WFR cannot be set in Mobile mode.
WF, R3000, IR or WFR target server:	No MSC-related menus are available. An IR or WFR cannot be set in Mobile mode.

Remote Filtering Components

Remote filtering components for using MSC include:

- Web Filter configured to use the Mobile mode for filtering mobile workstations, and the following setup:

  - Authentication enabled on the mobile Web Filter
  - IP group/user profiles and/or LDAP domain group/user profiles set up on the mobile Web Filter

    These settings ensure the mobile user's activity is logged by username and not by IP group/LDAP domain name. Without these settings, mobile user traffic will be logged under the "IPGROUP" or "DEFAULT" (Global Group) profile.

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

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, within minutes an administrator can generate customized reports showing the mobile 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 the aid of an external device in the communication process 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 in the communication process 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—containing IP group/user profiles and/or LDAP domain group/user profiles—gives the mobile Web Filter the group/domain 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. 1-1 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. 1-2 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.
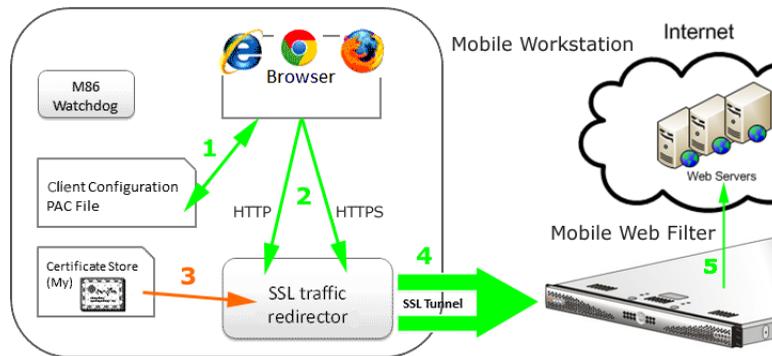
Fig. 1-3 Mobile workstation flow to mobile Web Filter (internal PAC file)

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 deter-mines 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 disal-lowed, the appropriate response is returned to the work-station.
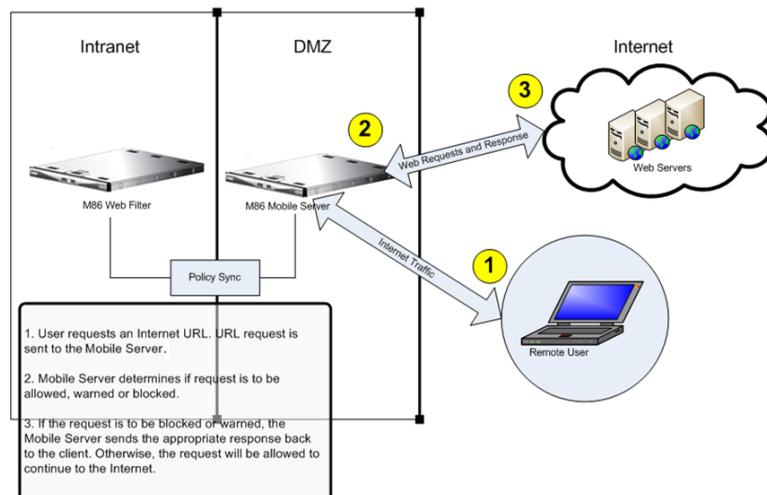
Fig. 1-4 Web Filters on and off premises, and workstation URL request

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.

PRELIMINARY SETUP

This portion of the user guide contains information on:

- Network setup information for using the mobile Web Filter.

- Mobile operation settings to specify the server will function as a mobile Filter.

- Enabling authentication and configuring pertinent settings.

- Specifying which device will create the MSC client, and issue, store, and manage certificates.

Network Setup Information

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.

- A server other than the mobile Web Filter can be designated to serve block pages to mobile users.

- 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

If using a non-IR or non-WFR Web Filter, 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":
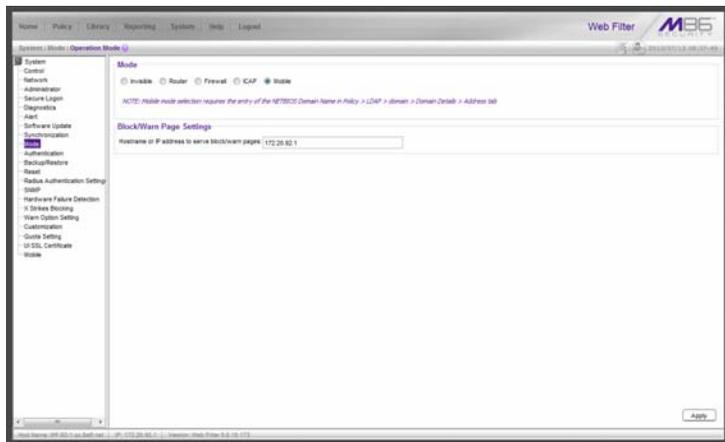
Fig. 2-1   Operation Mode window, Mobile mode

3. In the **Hostname or IP address to serve block/warn pages** field, the LAN1 IP address displays by default. This entry should be edited if a server other than the mobile Web Filter will serve warn pages and/or block pages to mobile users.

4. Click **Apply** to set the mobile mode and IP address; this action displays the Mobile menu topic in the System tree, with Certificate Management and Configuration subtopics, and the Certificate Management menu for IP groups and/or LDAP domains in the Policy tree.

NOTES: MSC-related menus in the System and Policy tree auto-matically display on a source server, whether or not that server is set in mobile mode.

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.

Mobile users who receive a block page will not have the options link which displays the Options page, since Web-based authenti-cation and override accounts are not supported in mobile filtering.

Enable Authentication, Configure Settings

Enable Authentication

In order for mobile user activity to be logged by profile name, the authentication feature must be enabled on the mobile Web Filter.

1. Navigate to System > Authentication > Enable/Disable Authentication:
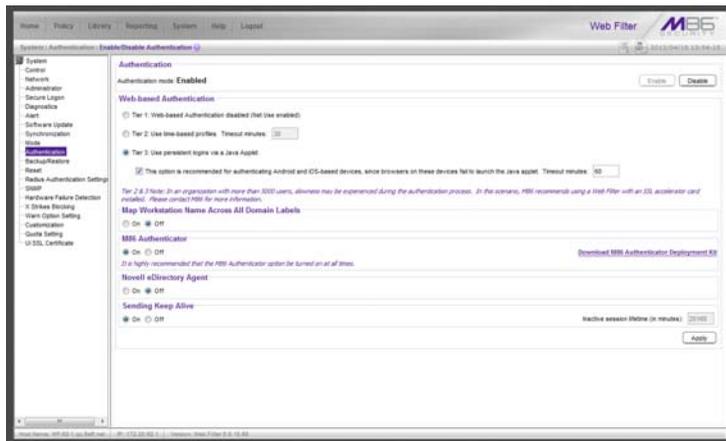
Fig. 2-2 Enable/Disable Authentication window

2. In the Authentication frame, click **Enable**.

NOTES: Users are authenticated based on the type of group in which their profile is stored: IP group or LDAP domain group.

Refer to the M86 Web Filter User Guide for Authentication for information on configuring and deploying authentication in your environment.

Set the NetBIOS Domain Name

If using an LDAP server in the authentication process, and the Web Filter will be generating, issuing, and managing all certificates, the NetBIOS domain name must be set for the LDAP domain.

1. Navigate to Policy > LDAP > domain > Domain Details > Address tab:

Fig. 2-3 LDAP Domain Details window, Address tab

2. Enter the **NETBIOS Domain Name** of the LDAP server—if this field is not populated—and then click **Save** and **Activate**.

NOTE: Refer to the M86 Web Filter User Guide for Authentication for information on configuring and deploying authentication in your environment.

Set the Certification Mode

On the mobile server—or the source server, in a synchronization environment with MSC—navigate to System > Mobile > Certificate Management to display the Certificate Management window:
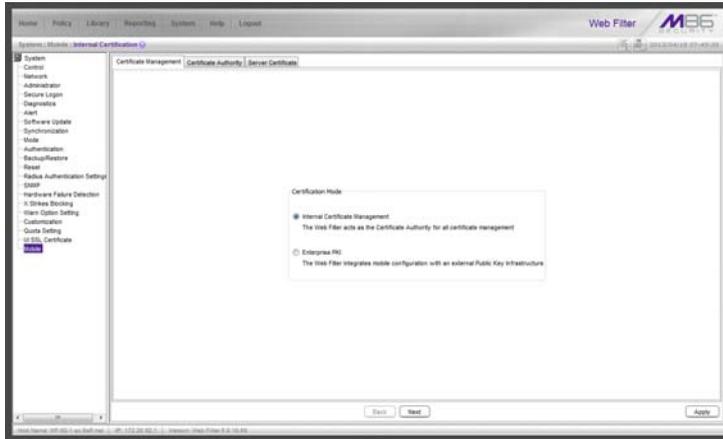
Fig. 2-4 Certificate Management window

Select the Certification Mode by choosing either the default "Internal Certificate Management" mode—if the Web Filter will issue and store certificates, or the "Enterprise PKI" mode—if an external device will issue and store certificates.

Based on this selection, different tabs display in this window. Proceed to instructions in the section of this user guide for the selected Certification Mode:

• Internal Certificate Management

• Enterprise PKI

INTERNAL CERTIFICATE MANAGEMENT

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

Configure Mobile Server, Client Settings

The first step in setting up MSC in the internal mode is to use the Certificate Management wizard to generate certificates to be stored on this mobile Web Filter.

The second step is to use the Configuration wizard to create the Proxy Auto-Configuration (PAC) file that 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—which also contains a generic client certificate—for ready deployment to end user mobile workstations.

A third step is required only if any mobile user will be issued a unique user certificate. For this step, mobile IP group and/or LDAP domain users are set up receive unique certificates and to have these certificates managed by the mobile Web Filter.

Generate Certificates

In System > Mobile > Certificate Management window, the "Internal Certificate Management" option should have been selected:
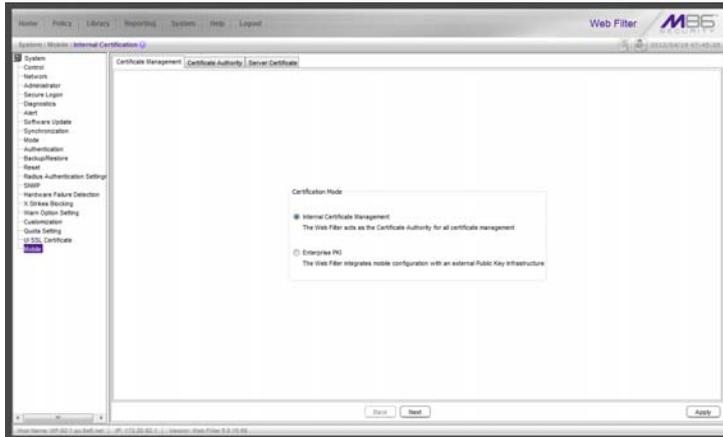
Fig. 3-1 Certificate Management window, internal option

Certificate criteria is set up using the remaining tabs in the Certificate Management wizard.

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

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

Step A: Generate the CA Certificate

The Certificate Authority tab is used for generating the CA certificate for this mobile Web Filter designated to generate and issue certificates to mobile users.
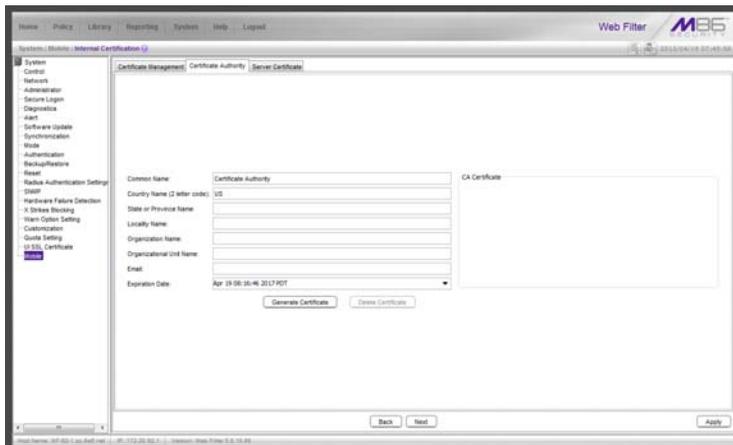
Fig. 3-2 Certificate Authority tab

By default, the only populated fields include Common Name, Country Name (2 letter code), and Expiration Date—defaulted to five years from this point in time. Filling in the rest of the fields is optional.

1. At your option, edit or type in your entries in the following fields:

   a. **Common Name**: "Certificate Authority" displays by default.

   b. **Country Name (2 letter code)**: Your two-character country code displays by default.

   c. **State or Province Name**: Full name or code identifying your state or province, such as *CA* or *California*.

   d. **Locality Name**: Name of your organization's city or principality, such as *Irvine*.

e. **Organization Name**: Name of your organization, such as *Logo Corporation*.

f. **Organizational Unit Name**: Name of your department, such as *Administration*.

g. **Email**: Your email address.

2. The **Expiration Date** field displays the date and time five years 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 Certificate** to generate the server certificate. The successfully generated certificate populates the CA Certificate box to the right with the contents of the certificate:
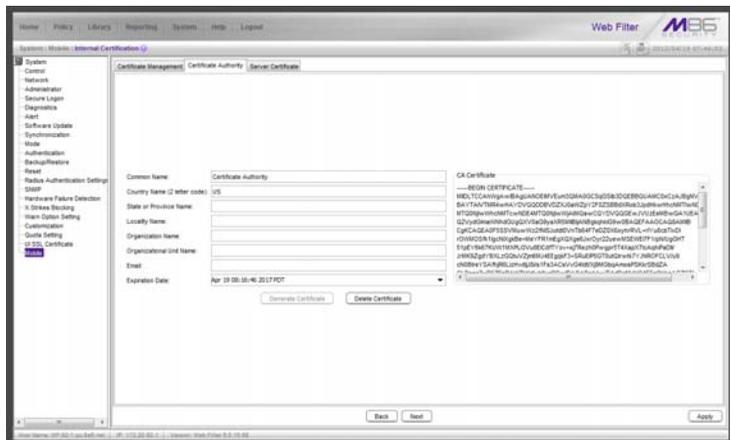
Fig. 3-3 Generated CA Certificate

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

4. Click **Next** to go to the Server Certificate tab to generate the server certificate.

Step B: 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. 3-4 Server Certificate tab

By default, the entries made in the fields in the Certificate Authority tab populate the fields by the same name in the Server Certificate name tab, except for the Common Name field, which displays the host name of the mobile Web Filter.

*NOTE: By default, the Generate Certificate button displays greyed-out. Click **Delete Certificate** if any criteria previously specified in this tab has changed and you need to generate a new certificate.*

Click **Apply** to save your settings.

Re-Generate a Server Certificate

1. If you need to re-generate the Server Certificate, 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 Name**: Full name or code identifying your state or province, such as *CA* or *California*.

   d. **Locality Name**: Name of your organization's city or principality, such as *Irvine*.

   e. **Organization Name**: Name of your organization, such as *Logo Corporation*.

   f. **Organizational Unit Name**: Name of your department, such as *Administration*.

   g. **Email**: Your email address.

2. The **Expiration Date** field displays the date and time five years 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 Certificate** to generate the server certificate. The successfully generated certificate populates the Certificate Signing Request box to the right with the contents of the certificate:

4. Click **Apply** to save your settings.

Configure the Client

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

Fig. 3-5 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**.*

Step A: 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 **Hostname** 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, the default **Enhanced Key Usage** number displays. If necessary, modify this code the MSC client will use in order to identify the user certificate for connecting to the mobile Web Filter.

7. Click **Next** to go to the Client Options tab.

Step B: Set Global Password, Client Options

The Client Options tab is used for setting the global password for unique client certificates, and indicating which optional features will be included in the client.
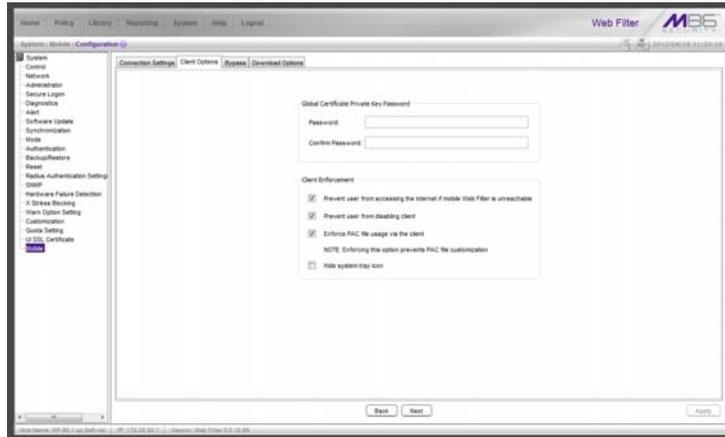
Fig. 3-6 Client Options tab

1. In the Global Certificate Private Key Password frame, make the same entry in the **Password** and **Confirm Password** fields for the password mobile users will use if installing unique client certificates issued to them.

NOTE: *The Global Certificate Private Key Password feature is only used for unique, non-generic user certificates.*

2. In the Client Enforcement frame, 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.

3. Click **Next** to go to the Bypass tab.

Step C: 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. 3-7 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 **Remove**.*

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.

Step D: Download the Client Installer or PAC File

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

Fig. 3-8 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.

Set Up, Manage Unique User Certificates

NOTE: Instructions in this sub-section need to be followed only if issuing unique, non-generic user certificates to mobile users. This sub-section can be skipped if all mobile users will be using the generic mobile user certificate.

The process of setting up unique, non-generic mobile user certificates differs between IP groups and LDAP domains.

Before user certificates can be issued to mobile users in IP groups, these users must first be added to the IP group's Certificate Management table. For LDAP domains, users must be imported from the LDAP server into the LDAP domain's Certificate Management table.

Once mobile users are included in the Certificate Management table, certificates for these users can be issued or re-issued, emailed, exported or revoked.

This sub-section describes certificate setup for IP groups and LDAP domains, followed by certificate management for both IP groups and LDAP domains.

Certificate Management Setup

Proceed to the appropriate section to set up user certificates for management: IP Group, or LDAP Domain.

Certificate Management window for IP group

Navigate to Policy > IP group and select Certificate Management from the menu to display the Certificate Management window:
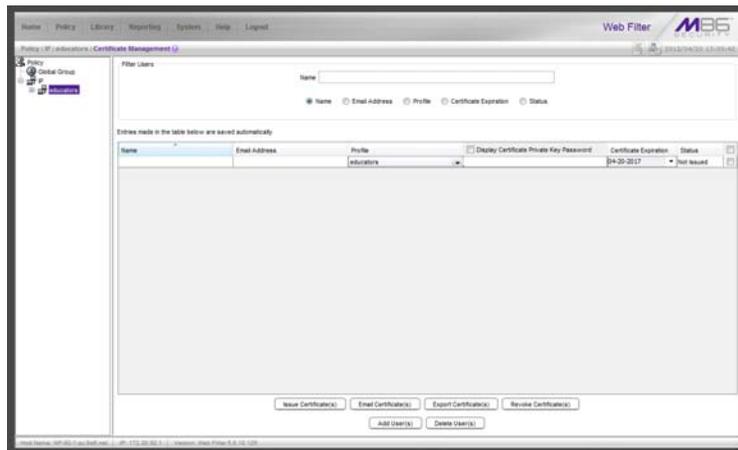
Fig. 3-9 Certificate Management for IP group, row of users added

This window is used for adding IP group mobile users for certificate management, and contains the Filter Users frame for filtering a user search, a table below for managing user certificates, and a row of buttons at the bottom for executing tasks.

NOTE: Entries made in the table are saved automatically.

Set up Users for Certificate Management

1. Click **Add User(s)** to add a row of IP group users to the table (see Fig. 3-10). This entry displays a name in the Profile column (either a user name or the IP group name), a Certificate Expiration date five years from this point in time, and a "Not Issued" Status.

NOTE: See Manage Certificates: Issue Certificates in this section for instructions on issuing mobile user certificates.

2. In the Profile column, use the pull-down menu to select the user to be issued a mobile user certificate, or use the IP group profile if the user profile has not been set up in that node.

3. For that user:

   a. Enter the user's **Name** as it will appear in the salutation of the certificate installation instructions of the email message. The user's Name can be edited as long as the certificate has not yet been issued.

TIP: The Name should contain no breaks; use the underscore "_" character to add a space between first and last name.

   b. Enter the user's **Email Address**.

   c. Entering a password is optional. By default, passwords display encrypted in this column, but can be made visible by clicking "Display Certificate Private Key Password" above this column. A password can be edited as long as the certificate has not yet been issued. If no password is entered, the user will use the global password set up in the Global Certificate Private Key Password fields in System > Mobile > Configuration > Client Options tab.

d. By default, **Certificate Expiration** displays a date five years from this point in time using the MM-DD-YYYY format. This date can be changed by clicking the down arrow and choosing a new future date—at least a day from today—in the pop-up calendar. The expiration date can be modified as long as the certificate has not yet been issued.

e. By default, "Not Issued" displays for the certificate **Status**. This status changes when the certificate is issued, emailed, expired, or revoked.

*NOTE: To delete any user(s) from the table, click the checkbox(es) in the far right column at the end of the row, and then click **Delete User(s)**.*
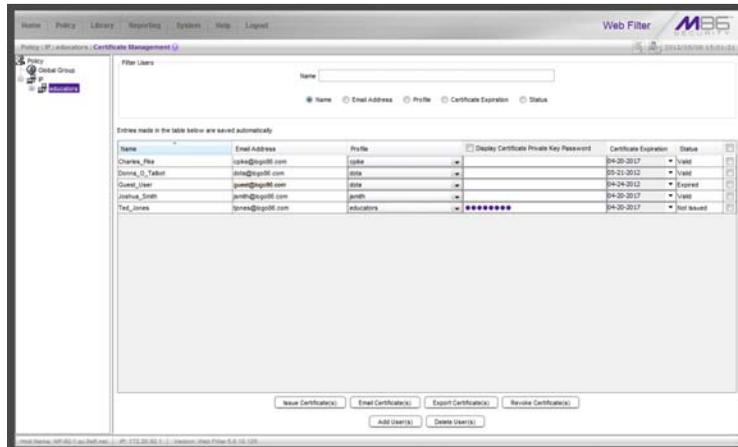
Fig. 3-10 Certificate Management window, IP group users added

Follow the instructions in this sub-section for each user to be added to the Certificate Management table.

Proceed to Manage Users in the table.

Certificate Management window for LDAP domain

Navigate to Policy > LDAP domain and select Certificate Management from the menu to display the Certificate Management window:
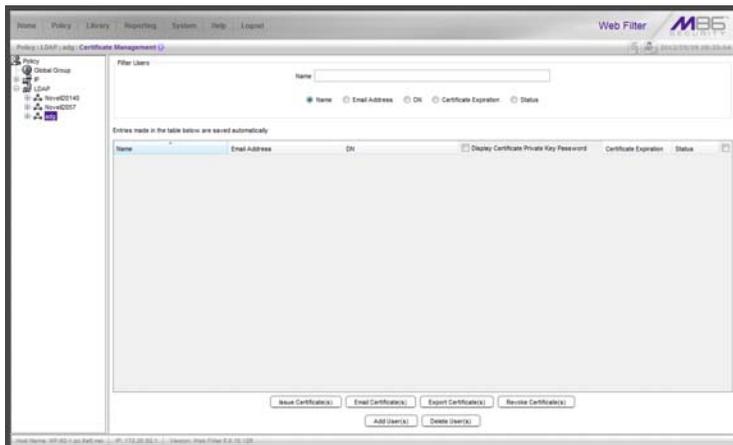
Fig. 3-11 Certificate Management window for LDAP domain

This window is used for importing LDAP domain mobile users for certificate management, and contains the Filter Users frame for filtering a user search, a table below for managing user certificates, and a row of buttons at the bottom for executing tasks. Though similar to the IP group window of the same name, the Profile radio button and column for IP groups are replaced by the DN (Distinguished Name) radio button and column for LDAP domains.

Import Users for Certificate Management

Click **Add User(s)** to go to the LDAP Browser window where you query the domain for users to be imported to the Certificate Management table:
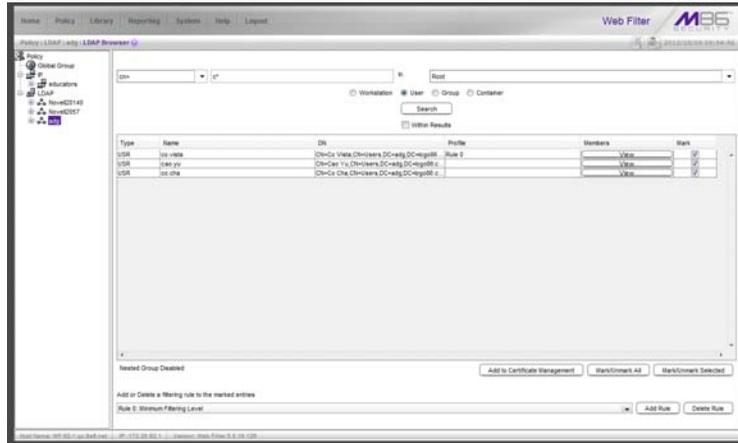
Fig. 3-12 LDAP Browser window

Perform a basic search

1. Select "User" and choose either "cn=" (common name) or "uid=" (user ID) from the pull-down menu for the attribute type used in the LDAP directory.

2. In the input field that follows the pull-down menu, type in the username exactly as it was entered on the LDAP server, or enter a partial name followed by the asterisk (*) wildcard.

3. Make a selection from the **In** pull-down menu to specify the section of the server to search.

4. Click **Search** to display rows of results in the table below. The following information is included for each entity: Type (USR), Name (as entered on the LDAP server), DN (Distinguished Name) string, Profile (Rule number, if

assigned), View button in Members column, and Mark checkbox.

Options for search results

The following actions can be performed on search results:

- To narrow the number of records returned by your initial query, click the "Within Results" checkbox, modify your search criteria in the input field, and then click **Search**.

- To query either the list of groups in which a user is a member, or the list of users who are members of a Group Record, click the **View** button in the Members column to display the results in the table.

- To select or deselect all records in the table, click **Mark/ Unmark All**.

- To select or deselect all highlighted records in the table, click **Mark/Unmark Selected**. This feature works only if records are first selected in the table by clicking on them.

  - Multiple records are selected by clicking one record, and then pressing the **Ctrl** key on your keyboard and clicking another record.

  - A block of multiple records is selected by clicking the first record in the block, then pressing the **Shift** key on your keyboard, and then clicking the last record in the block.

Add user(s) to the Certificate Management table

To add the user(s) to the Certificate Management table:

1. Go to the Mark column and click the checkbox(es) for the selected user(s).

2. Click **Add to Certificate Management**.

3. Go to the Certificate Management window to view the users imported into the Certificate Management table:
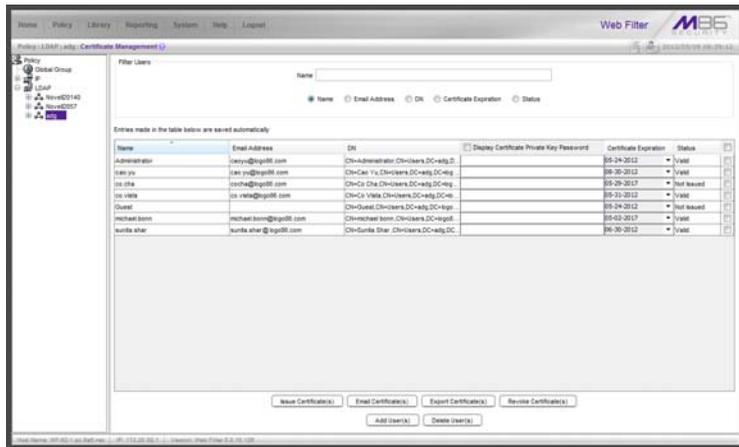
Fig. 3-13 Certificate Management window with LDAP users imported

NOTE: *To delete any user(s) from the table, click the checkbox(es) in the far right column at the end of the row, and then click* ***Delete User(s)***.

Proceed to Manage Users in the table.

Manage Users in the table

Once users are added to the Certificate Management table, certificates can be issued, re-issued, or revoked, as necessary. Proper maintenance on this table ensures that only valid mobile users have online access via their mobile workstations.

To help you manage user certificates, the table can be sorted by various columns, and/or filtered.

Sort the Certificate Management table

By default, the table is sorted in ascending order by the Name column, but can be re-sorted in descending order by clicking the Name column header. To sort the table by another column, click the column header in this same manner for Email Address, Profile (for IP groups only) or DN (for LDAP domains only), Certificate Expiration, or Status.

Filter Users frame and Certificate Management table

In the Filter Users frame, by default the "Name" radio button is enabled and the Name field displays along with all users in the table. Use a radio button and fields to display query results in the table as follows:

Name

If not enabled, click the "Name" radio button to display the **Name** field in which characters for a user's name are input. Results immediately display in the table based on consecutive, matching character entries found among all names set up for this node. For IP group users, the user's Name can be edited as long as a certificate has not yet been issued.

Email Address

Click the "Email Address" radio button to display the **Email Address** field in which characters for a user's email address are input. Results immediately display in the table based on consecutive, matching character entries found among all email addresses set up for this node. The user's Email Address is editable in the event it has changed since the last time a certificate was issued.

Profile (for IP groups only)

For the IP group, click the "Profile" radio button to display the **Profile** field from which the user's profile is selected from the pull-down menu. By default "All Profiles" displays.

DN (for LDAP domains only)

For the LDAP domain, click the "DN" radio button to display the **DN** field in which characters for a user's Distinguished Name are input. Results immediately display in the table based on consecutive, matching DN character entries found among all users set up for this node.

Certificate Expiration

Click "Certificate Expiration" to display the range of certificate expiration dates (using the MM-DD-YYYY format) **From** five years prior **To** five years from today. Calendar dates are modified by clicking the down arrow to open the calendar pop-up box and selecting another date. Results immediately display in the table based on all user certificates set up for this node found to have expiration dates that fall within the specified date range. The Certificate Expiration date can only be modified if the certificate has not yet been issued.

Status

Click the "Status" radio button to display the **Status** field from which the user's certificate status is selected from the pull-down menu. By default "All Status" displays. Selecting the following certificate status type displays all users set up for this node found to have the corresponding certificate status: "Not Issued", "Valid", "Expired", or "Revoked".

Update Users in the table

IP group user updates

For IP group mobile users added to the Certificate Management table, updates to all fields except Status (Name, Email Address, Profile, password, Certificate Expiration—see Set up Users for Certificate Management) can be made as long as certificates have not yet been issued.

Once a certificate is issued, only the following fields can be modified:

• **Email Address** - Enter the updated email address.

• **Profile** - Select the Profile from the pull-down menu.

To delete the user(s), click the checkbox at the end of the row, and then click the **Delete User(s)** button beneath the table.

LDAP domain user updates

For LDAP domain mobile users imported into the Certificate Management table, edits can only be made to the following fields:

- **Email Address** - Enter the user's email address.

- password - This entry is optional. By default, passwords display encrypted in this column, but can be made visible by clicking "Display Certificate Private Key Password" above this column. A password can be edited as long as the certificate has not yet been issued. If no password is entered, the user will use the global password set up in the Global Certificate Private Key Password fields in System > Mobile > Configuration > Client Options tab.

- **Certificate Expiration** - By default, this field displays a date five years from this point in time using the MM-DD-YYYY format. This date can be changed by clicking the down arrow and choosing a new future date—at least a day from today—in the pop-up calendar. The expiration date can be modified as long as the certificate has not yet been issued.

Once a certificate is issued, only the Email Address field can be edited.

To delete the user(s), click the checkbox at the end of the row, and then click the **Delete User(s)** button beneath the table.

Manage Certificates

This sub-section describes the certificate Status types and actions to perform when managing mobile user certificates.

Certificate Status types

The following Status types display for certificates meeting that criterion:

- **Not Issued** - This certificate Status type displays for a certificate that has not yet been issued to the mobile user. A certificate with this status will not expire even if the Certificate Expiration date has passed.

- **Valid** - This certificate Status type displays for a certificate that has been issued to the mobile user and the Certificate Expiration date has not yet passed.

- **Expired** - This certificate Status type displays for a certificate that has been issued to a mobile user but has now expired, denoted by a past date in the Certificate Expiration column. A certificate with this status can be re-issued.

- **Revoked** - This certificate Status type displays for a certificate that had been issued to a mobile user but subsequently needed to be de-activated. A certificate with this status can be re-issued.

Validate a Mobile User, Issue a Certificate

To issue a certificate to a valid mobile user with a "Not Issued", "Expired", or "Revoked" Status:

1. Specify the **Certificate Expiration** date by clicking the down arrow and choosing a new future date—at least a full day and 24 hours from this point in time—in the pop-up calendar.

2. Click the checkbox at the end of the row.

3. Click **Issue Certificate(s)** beneath the table to change the certificate Status to "Valid."

Provide the Certificate for Installation

A valid certificate can be emailed to the user to install on the mobile workstation, or downloaded by the administrator for installation on the user's mobile workstation.

Email the Certificate to the Mobile User

For each "Valid" mobile user to be emailed the certificate to install on his/her mobile workstation:

1. Click the checkbox in the far right column.

2. Click **Email Certificate(s)** beneath the table to send the user two emails:

   • an email with the certificate attached contains instructions for installing the certificate

   • another email containing the private key password to use during the certificate installation process

TIP: This private key password comes from the mobile user's password field in the Certificate Management table, or the Global Certificate Private Key Password from the System > Mobile > Configuration > Client Options tab—the latter if no password was entered for the mobile user.

Download Certificates for Administrator Installation

If the administrator will be installing certificates on mobile workstations, he/she should do the following:

1. Click the checkbox(es) at the far right column for each "Valid" mobile user who needs a certificate installed on his/her mobile workstation.

2. Click **Export Certificate(s)** to download a .zip file containing the certificate(s) for the selected mobile user(s).

3. Extract the certificate(s) from this file.

4. Install the certificate(s) on the mobile user workstation(s) using the private key password for that mobile user.

TIP: This private key password comes from the mobile user's password field in the Certificate Management table, or the Global Certificate Private Key Password from the System > Mobile > Configuration > Client Options tab—the latter if no password was entered for the mobile user.

Revoke Certificates

To change the status of a mobile user certificate so that it is no longer "Valid", the certificate needs to be revoked. To revoke a "Valid" certificate:

1. Click the checkbox at the far right column for each mobile user certificate to be revoked.

2. Click **Revoke Certificate(s)** to change the mobile user certificate status to "Revoked".

ENTERPRISE PKI

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

Configure Mobile Server, Client Settings

The first step in setting up MSC in the external mode is to use the Certificate Management wizard to generate and import certificates into this mobile 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 those certificates are stored.

💡 *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".*

The second step 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

In System > Mobile > Certificate Management window, the "Enterprise PKI" option should have been selected:
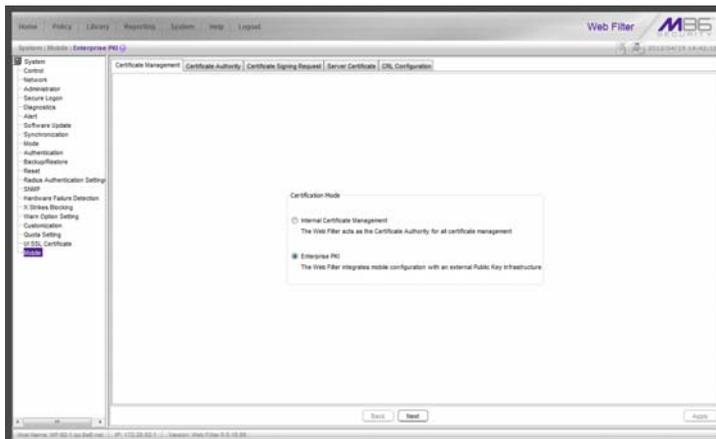
Fig. 4-1 Certificate Management window, Enterprise PKI option

Certificate criteria is set up using the remaining tabs in the Certificate Management wizard.

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

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

Step A: 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.
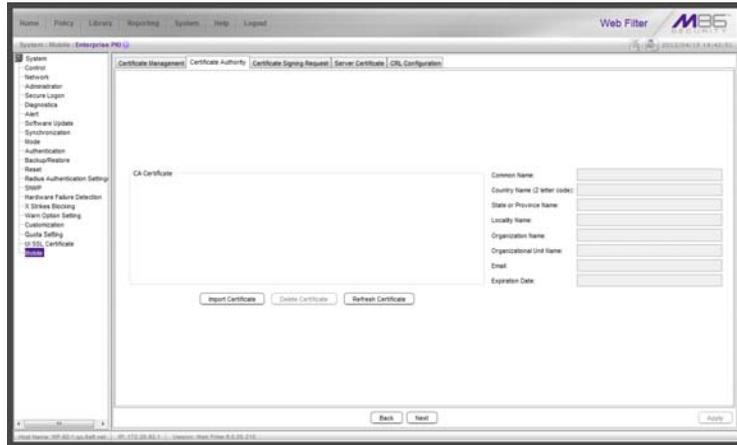
Fig. 4-2 Certificate Authority tab

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. 4-3 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 C.

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:
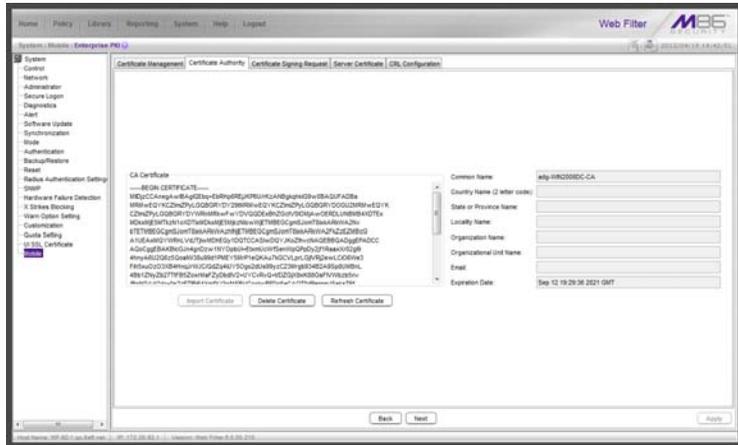
Fig. 4-4 Refreshed CA Certificate and window refreshed

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 C: 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.

NOTE: *The Delete Certificate button is activated when the window is refreshed. Click **Delete Certificate** if you need to import a new certificate.*

Step B: 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.
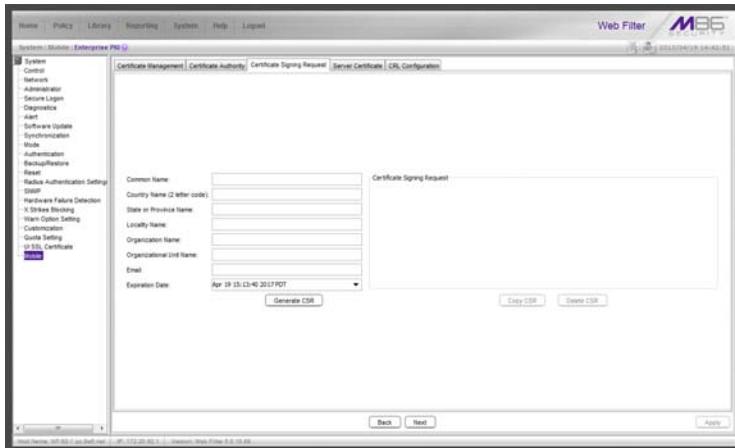
Fig. 4-5 Certificate Signing Request tab

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 Name**: Full name or code identifying your state or province, such as *CA* or *California*.

d. **Locality Name**: Name of your organization's city or principality, such as ***Irvine***.

e. **Organization Name**: Name of your organization, such as ***Logo Corporation***.

f. **Organizational Unit Name**: Name of your department, such as ***Administration***.

g. **Email**: Your email address.

2. The **Expiration Date** field displays a date and time five years 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:
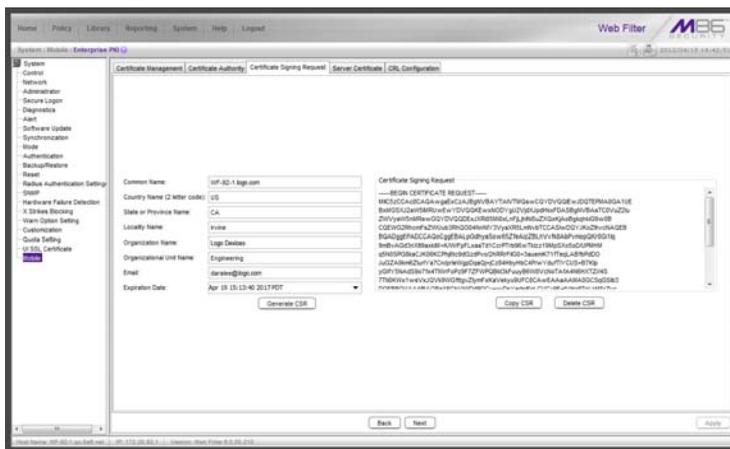
Fig. 4-6 Generated Certificate Signing Request

> *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 C: 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 C1: 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 C2: Import a Server Certificate.

Step C1: Import a CSR-based Certificate

1. Go to the Server Certificate tab:
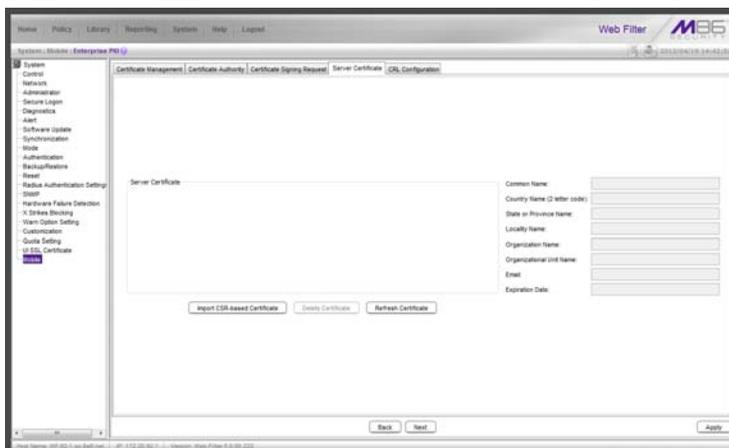
Fig. 4-7 Server Certificate tab for importing CSR-based certificate

Click **Import CSR-based Certificate** to open the CSR-based Server Certificate window/tab:
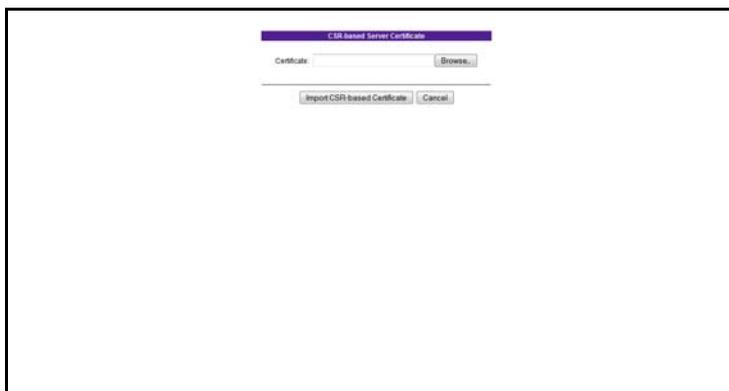
Fig. 4-8 CSR Certificate window

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:
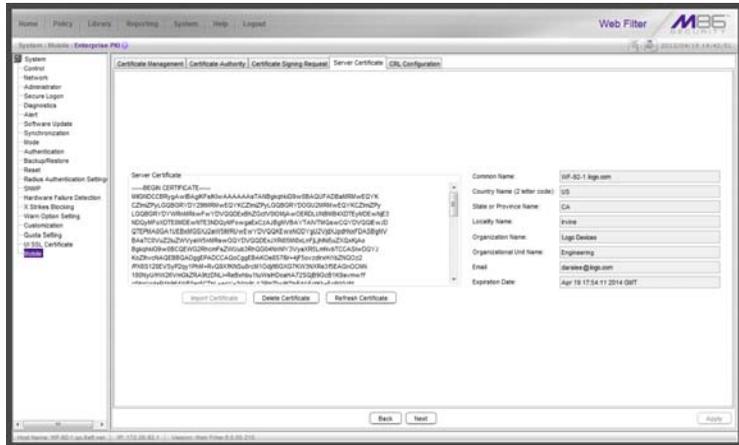
Fig. 4-9 Signed server certificate imported and window refreshed

*NOTE: The Delete Certificate button is activated when the window is refreshed. Click **Delete Certificate** if you need to import a new certificate.*

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

Step C2: Import a Server Certificate

1. Go to the Server Certificate tab:
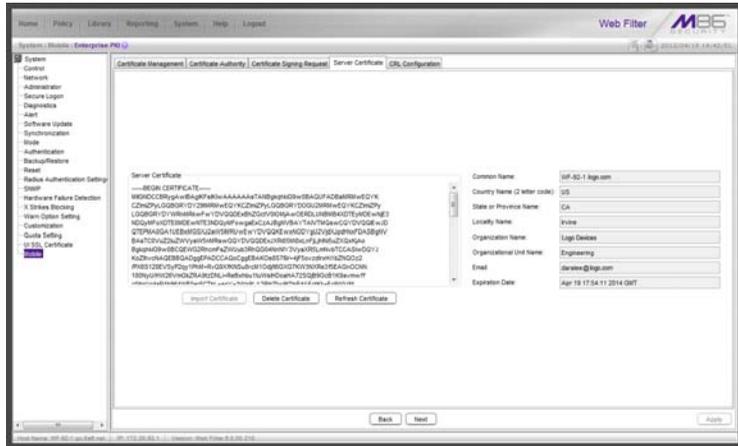
Fig. 4-10 Server Certificate tab for importing non-CSR certificate

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

Fig. 4-11 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.

Step D: 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.
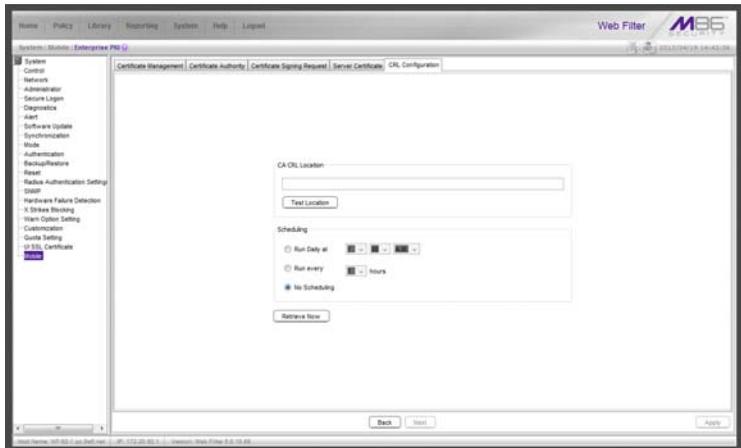
Fig. 4-12 CRL Configuration tab

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. 4-13 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-Config-uration (PAC) file can be downloaded for review and modifi-cation before deployment to end user workstations.

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

Step A: 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.

Step B: Specify Client Options

The Client Options tab is used for indicating which optional features will be included in the client.
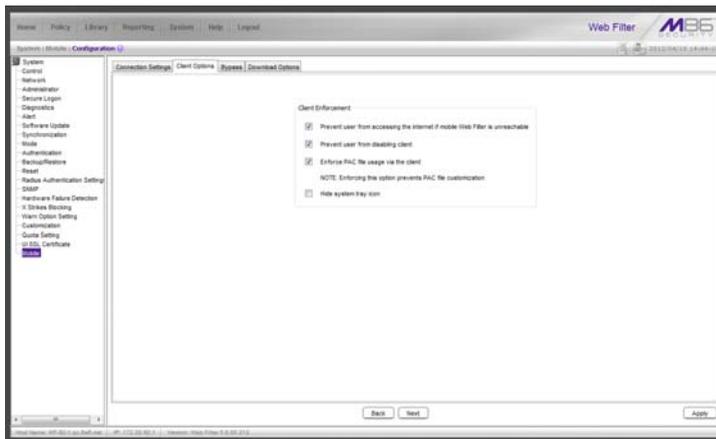
Fig. 4-14 Client Options tab

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.

Step C: 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.
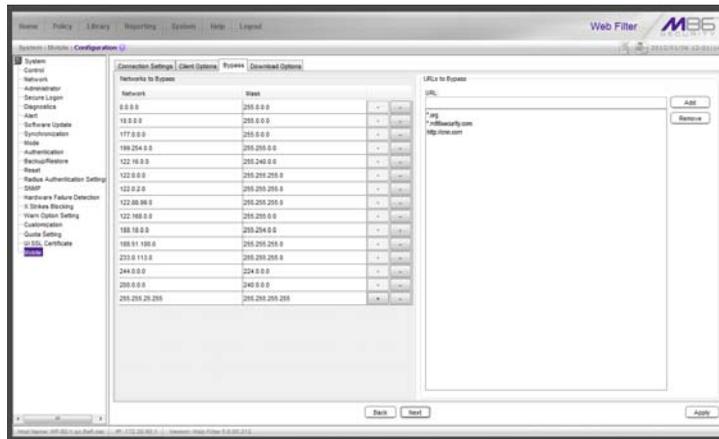
Fig. 4-15 Bypass tab

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 **Remove**.*

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.

Step D: Download the Client Installer or PAC File

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

Fig. 4-16 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:
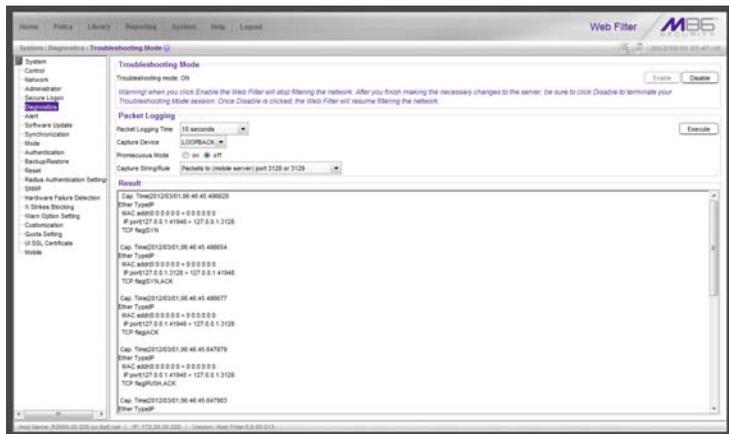
Fig. 5-1 Troubleshooting Mode window

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:

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

add IP users for Certificate Management *37*
administrator workstation requirements *3*

C

Certificate Management for IP groups *36*
Certificate Management for LDAP domains *39*
Certificate Management table sorting and filtering *43*
certificate status types *47*
certificates, types *8*
Certification Authority *8*
Certification Mode setup *20*
Certification Revocation List *60*
Certification Revocation List (CRL), definition *72*

D

DMZ *13*, *15*

E

email certificates to mobile users *48*
Enhanced Key Usage (EKU), definition *72*
Enterprise PKI, definition *72*
environment requirements *3*
export certificates for administrator installation *49*

F

Firefox *3*

G

Global Certificate Private Key Password *30*, *46*, *48*, *49*
Google Chrome *3*

I

import LDAP domain users for Certificate Management *40*
Internal Mode, definition *72*
Internet Explorer *3*
issue certificates to mobile users *48*

J

Java Plug-in *3*
Java Virtual Machine *3*
JavaScript *3*

L

Local Configuration Port, definition *72*

M

M86 Watchdog, definition *72*
Macintosh *3*

N

network requirements *4*

O

Operation Mode window
   mobile mode *16*

P

Proxy Auto-Configuration (PAC), definition *72*

R

remote filtering components *6*
reporting options *6*
revoke certificates *49*

S

Safari *3*
server certificate *8*
synchronization *5*
system requirements *3*

U

update users for Certificate Management *45*
user certificate *8*

W

Windows 7 *3*
Windows Vista *3*
Windows XP *3*