

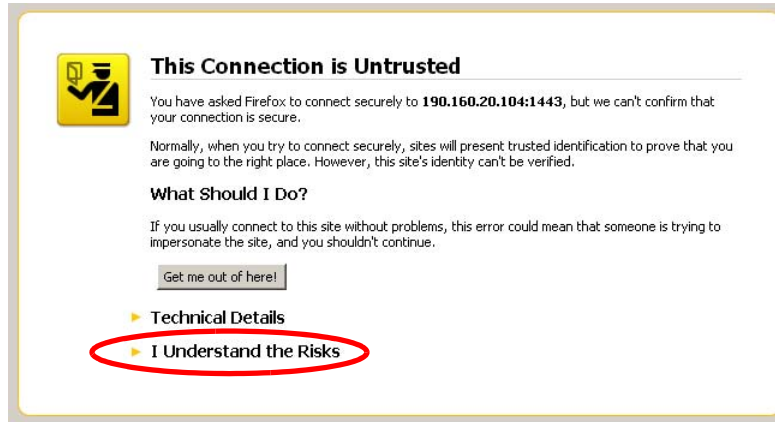
# ACCEPT THE SECURITY CERTIFICATE FOR WFR

## Access the WFR via its LAN 1 IP Address

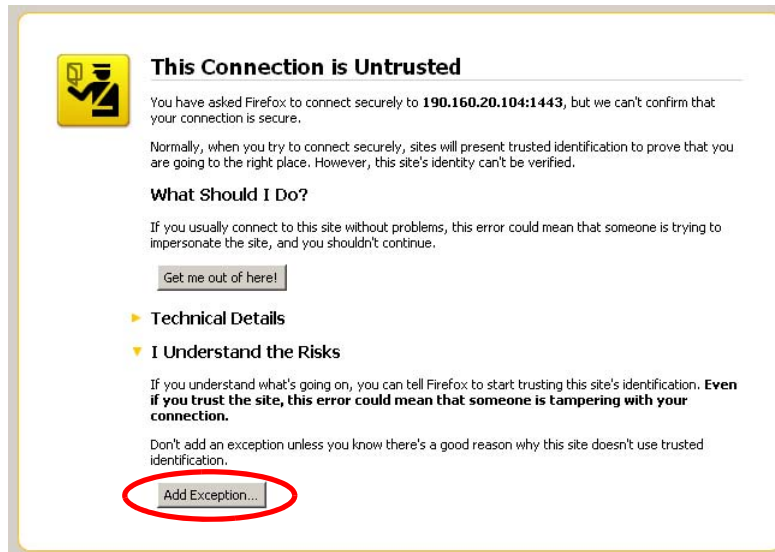
- A. Launch an Internet supported browser:
  - Firefox 9 or 10
  - Internet Explorer 8 or 9
  - Safari 5.0 or 5.1
  - Google Chrome 16 or 17
  
- B. In the address field, type in the LAN 1 IP address assigned to the WFR. Be sure to use “https” and port :1443 for a secure connection. For example, if the WFR were assigned an IP address of 10.10.10.10, you would enter **https://10.10.10.10:1443** in the browser’s address field.
  
- C. Click **Go** to display the security issue page:
  - If using Firefox, proceed to Accept the Security Certificate in Firefox.
  - If using IE, proceed to IE Security Certificate Installation Procedures.
  - If using Safari, proceed to Accept the Security Certificate in Safari.
  - If using Google Chrome, proceed to Accept the Security Certificate in Chrome.

# Accept the Security Certificate in Firefox

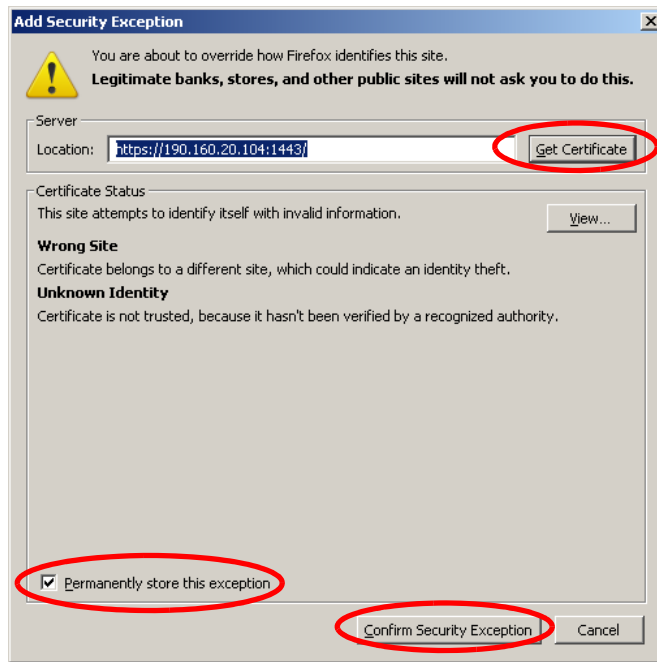
- A. If using a Firefox browser, in the page “This Connection is Untrusted,” click the option **I Understand the Risks**:



- B. In the next set of instructions that display, click **Add Exception...**:



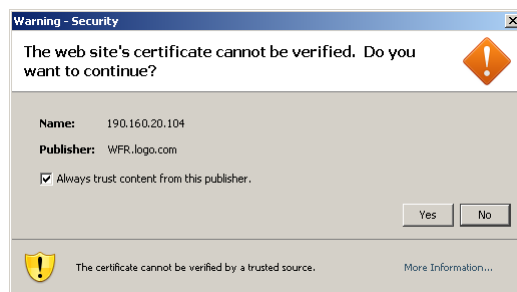
Clicking Add Exception opens the Add Security Exception window:



- C. In the Add Security Exception window, click **Get Certificate** and wait a few seconds until the security certificate is obtained by the server.
- D. With the checkbox **Permanently store this exception** selected, click **Confirm Security Exception** to open the WFR Welcome window:



**NOTE:** You will need to add a security exception for the Security Reporter when you attempt to access that application for the first time. On a newly installed unit, the SR Report Manager will remain inaccessible until logs are transferred to the SR and the SR's database is built.



When attempting to access the Web Filter user interface for the first time, the Security warning dialog box (shown in the sample image at left) will open instead of the Security Exception page. With the checkbox "Always trust content from this publisher." populated, click **Yes** to close the Security warning dialog box and to access the login window of the Web Filter user interface.

# IE Security Certificate Installation Procedures

## Accept the Security Certificate in IE

Go to the appropriate sub-section if using the following Windows operating system and IE browser:

- Windows XP or Vista with IE 8 or 9
- Windows 7 with IE 8 or 9

### Windows XP or Vista with IE 8 or 9

- A. If using an IE 8 or 9 browser on a Windows XP or Vista machine, in the page “There is a problem with this website's security certificate.”, click **Continue to this website (not recommended)**:

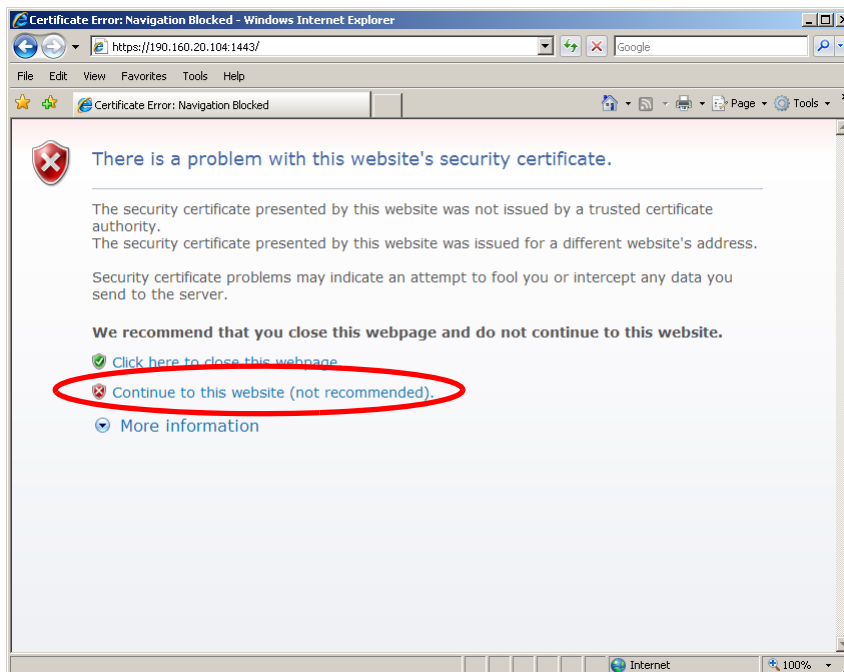


Figure A1: Windows XP, IE 8

Selecting this option displays the WFR Welcome window with the address field and the Certificate Error button to the right of the field shaded a reddish color:

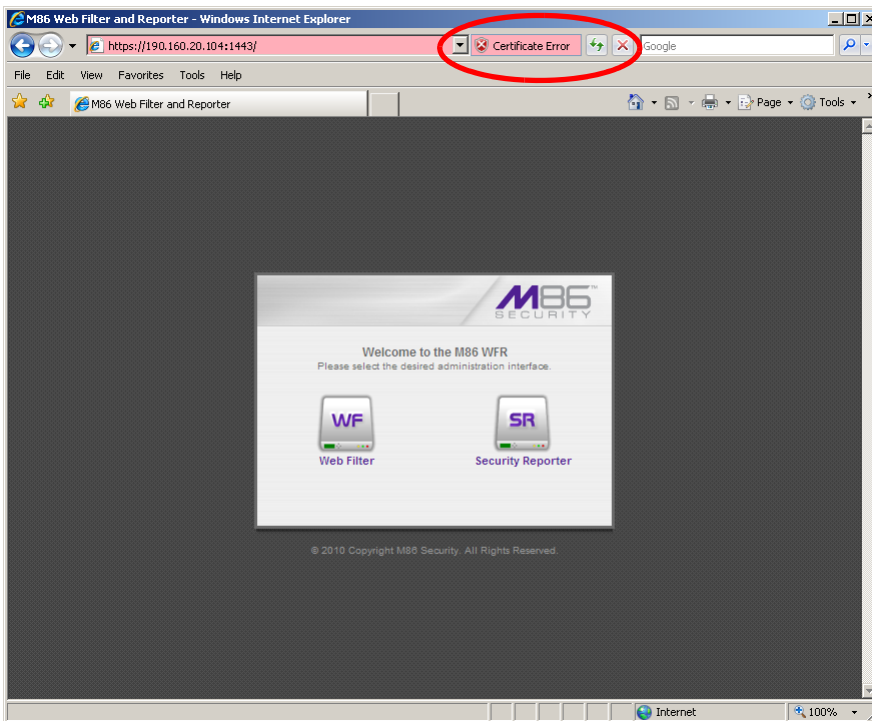


Figure A2: Windows XP, IE 8

B. Click **Certificate Error** to open the Certificate Invalid box:

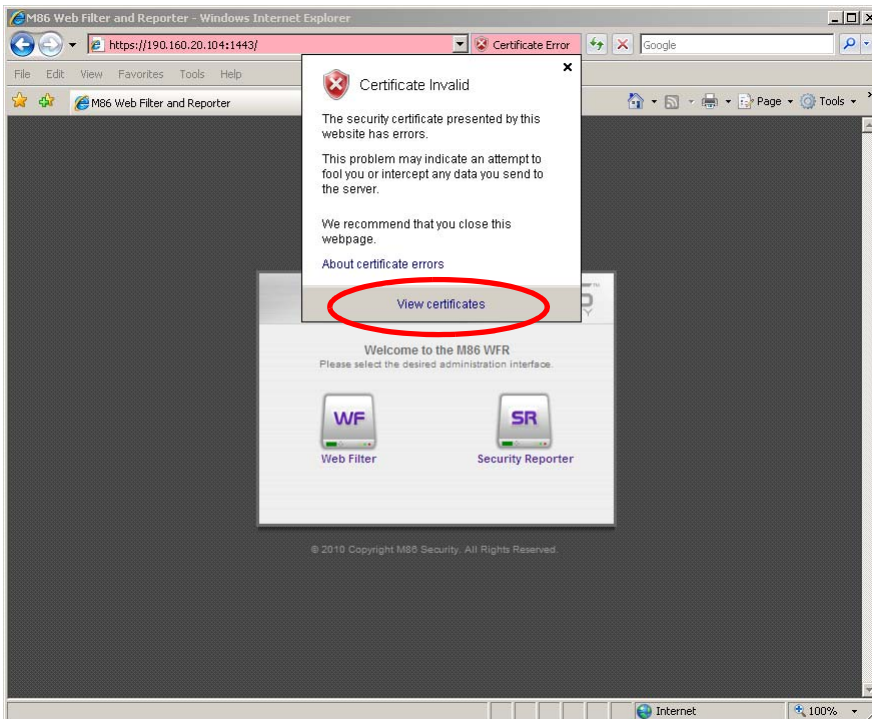


Figure B: Windows XP, IE 8

C. Click **View certificates** to open the Certificate window that includes the host name you assigned to the WFR:

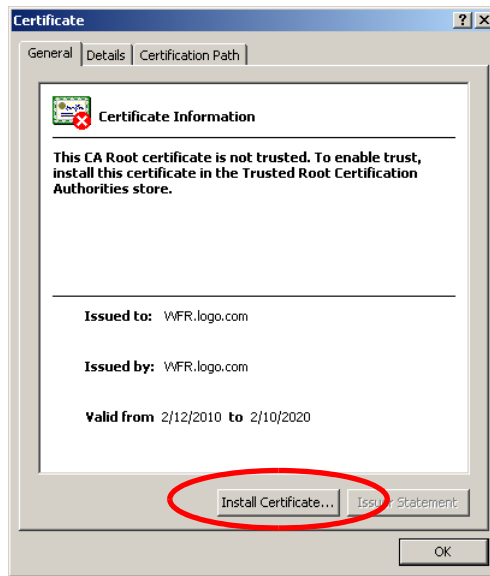


Figure C: Windows XP, IE 8

D. Click **Install Certificate...** to launch the Certificate Import Wizard:

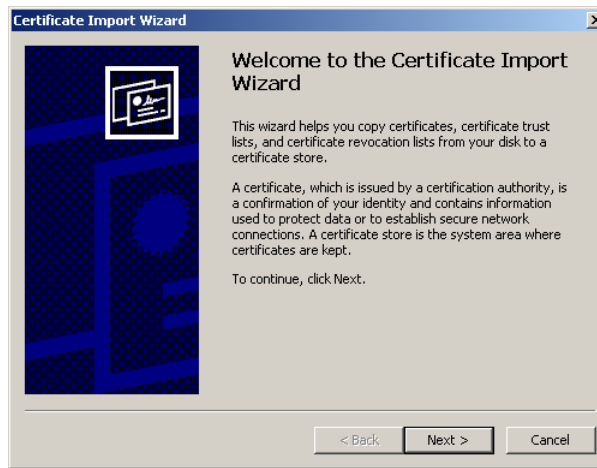


Figure D: Windows XP, IE 8

E. Click **Next >** to display the Certificate Store page:

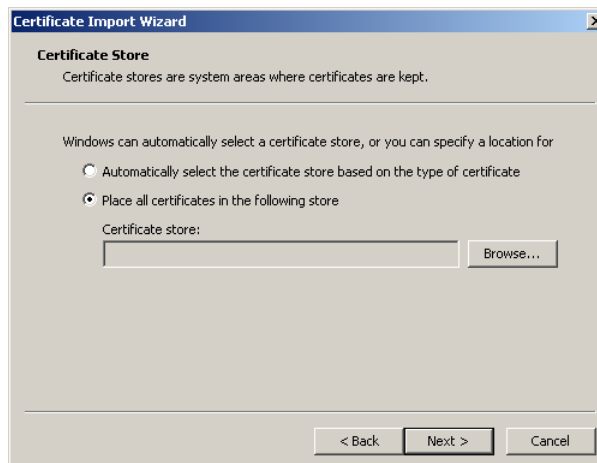


Figure E: Windows XP, IE 8

- F. Choose the option “Place all certificates in the following store” and then click **Browse...** to open the Select Certificate Store box:

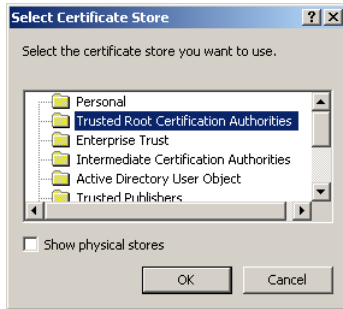


Figure F: Windows XP, IE 8

- G. Choose “Trusted Root Certification Authorities” and then click **OK** to close the box.
- H. Click **Next >** to display the last page of the wizard:

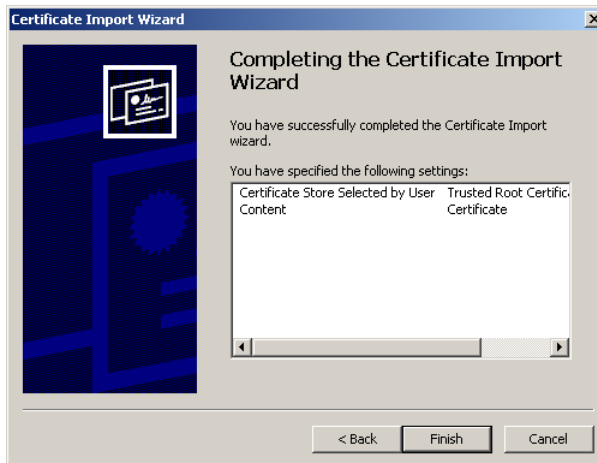


Figure H: Windows XP, IE 8

- I. Click **Finish** to close the wizard and to open the Security Warning dialog box asking if you wish to install the certificate:

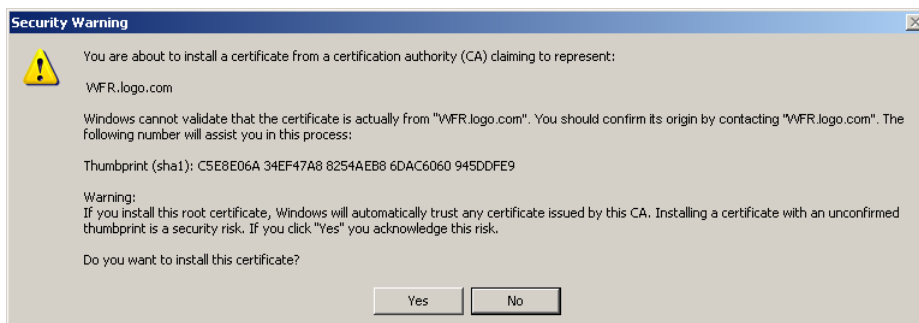


Figure I: Windows XP, IE 8

- J. Click **Yes** to install the certificate and to close the dialog box. When the certificate is installed, the alert window opens to inform you the certificate installation process has been completed.
- K. Click **OK** to close the alert box, and then close the Certificate window.

Now that the security certificate is installed, you will need to map the WFR's IP address to its host name. Proceed to Map the WFR's IP Address to the Server's Host Name.

## Windows 7 with IE 8 or 9

---

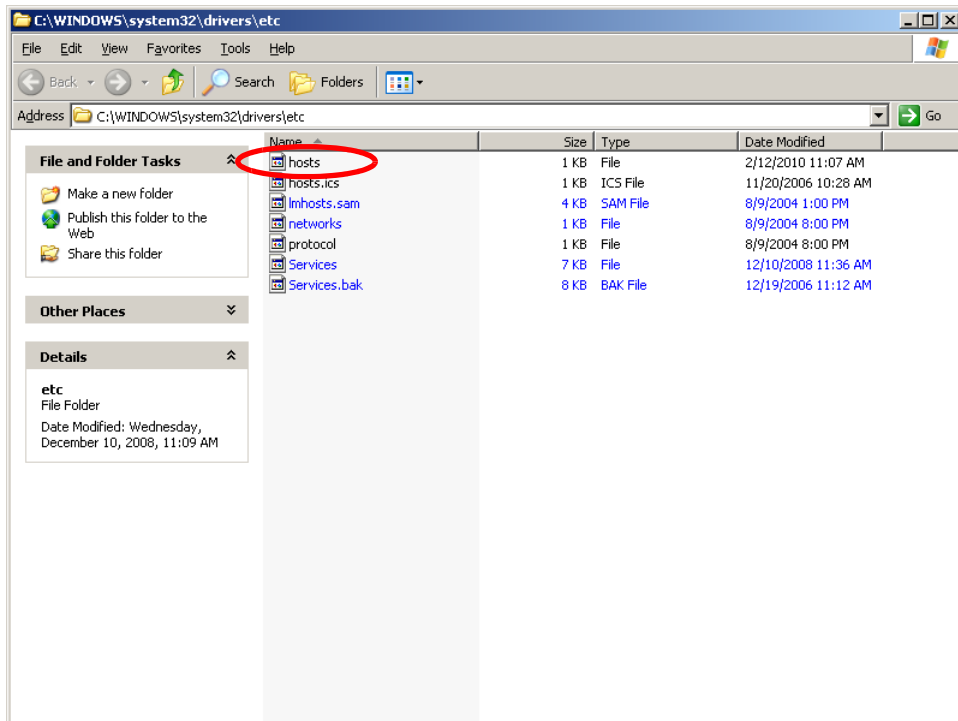
- A. If using an IE 8 or 9 browser on a Windows 7 machine, in the page "There is a problem with this website's security certificate.", click **Continue to this website (not recommended)**.
- B. From the toolbar, select **Tools > Internet Options** to open the Internet Options box.
- C. Select the Security tab, click **Trusted sites**, and then click **Sites** to open the Trusted sites box.
- D. In the Trusted sites box, confirm the URL displayed in the field matches the IP address of the WFR, and then click **Add** and **Close**.
- E. Click **OK** to close the Internet Options box.
- F. Refresh the current Web page by pressing the **F5** key on your keyboard.
- G. Follow steps A to K documented in Windows XP or Vista with IE 8 or 9:
  - When the security issue page re-displays with the message: "There is a problem with this website's security certificate.", click **Continue to this website (not recommended)** (see Figure A1). Choosing this option displays the WFR Welcome window with the address field and the Certificate Error button to the right of the field shaded a reddish color (see Figure A2).
  - Click **Certificate Error** to open the Certificate Invalid box (see Figure B).
  - Click **View certificates** to open the Certificate window that includes the host name you assigned to the WFR (see Figure C).
  - Click **Install Certificate...** to launch the Certificate Import Wizard (see Figure D).
  - Click **Next >** to display the Certificate Store page (see Figure E).
  - Choose the option "Place all certificates in the following store" and then click **Browse...** to open the Select Certificate Store box (see Figure F).
  - Choose "Trusted Root Certification Authorities" and then click **OK** to close the box.
  - Click **Next >** to display the last page of the wizard (see Figure G).
  - Click **Finish** to close the wizard and to open the Security Warning dialog box asking if you wish to install the certificate (see Figure H).
  - Click **Yes** to install the certificate and to close the dialog box. When the certificate is installed, the alert window opens to inform you the certificate installation process has been completed (see Figure I).
  - Click **OK** to close the alert box, and then close the Certificate window.
- H. From the toolbar of your browser, select **Tools > Internet Options** to open the Internet Options box.
- I. Select the Security tab, click **Trusted sites**, and then click **Sites** to open the Trusted sites box.
- J. Select the URL you just added, click **Remove**, and then click **Close**.



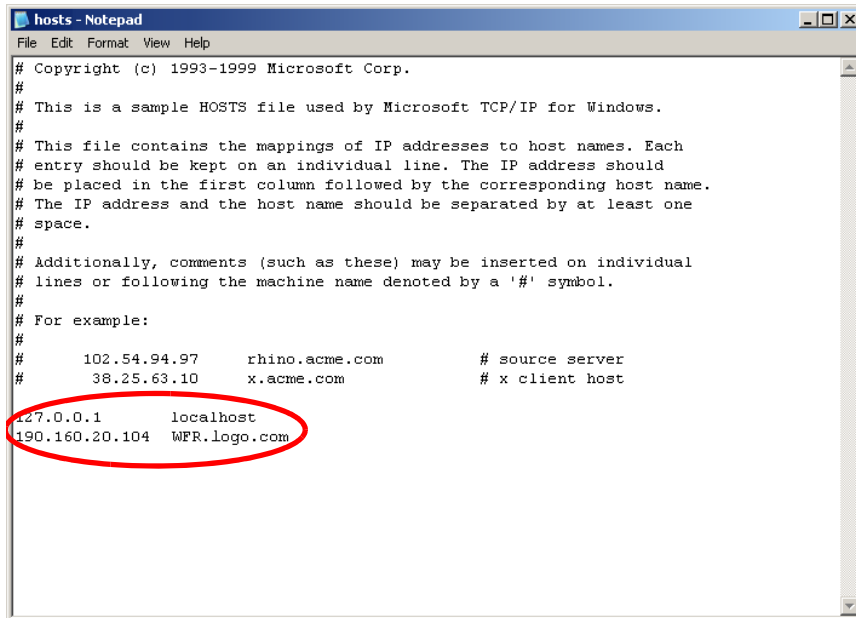
Now that the security certificate is installed, you will need to map the WFR's IP address to its host name. Proceed to Map the WFR's IP Address to the Server's Host Name.

## Map the WFRs IP Address to the Server's Host Name

- A. From your workstation, launch Windows Explorer and enter **C:\WINDOWS\system32\drivers\etc** in the Address field to open the folder where the hosts file is located:

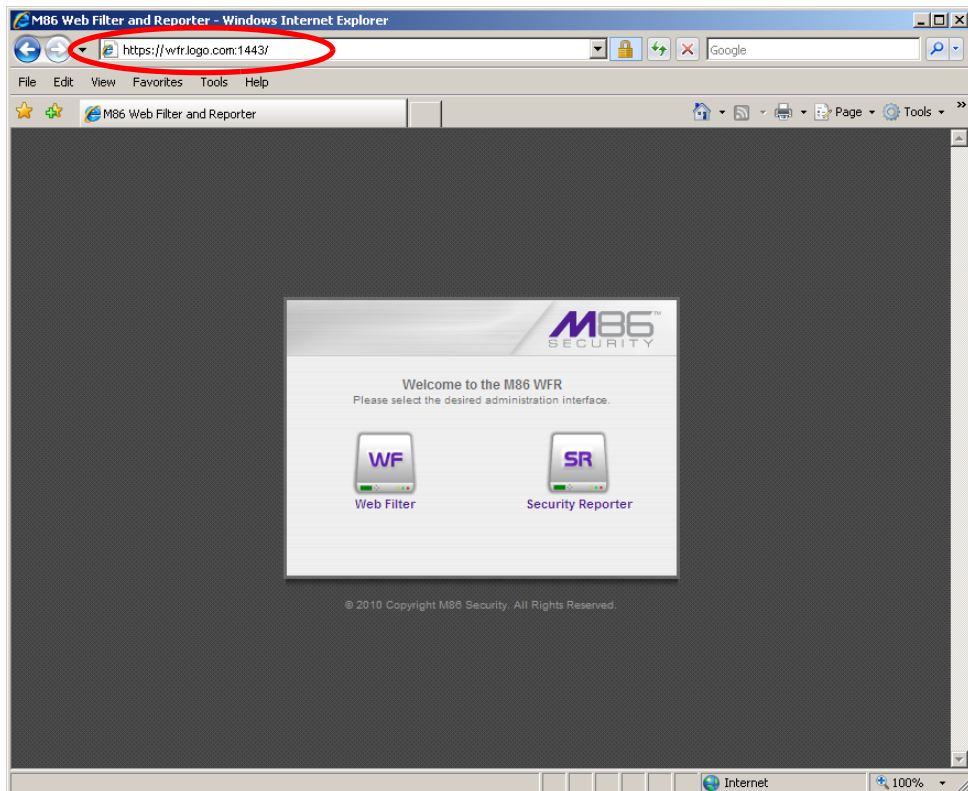


- B. Double-click "hosts" to open a window asking which program you wish to use to open the file. Double-click "Notepad" or "TextPad" to launch the hosts file using that selected program:



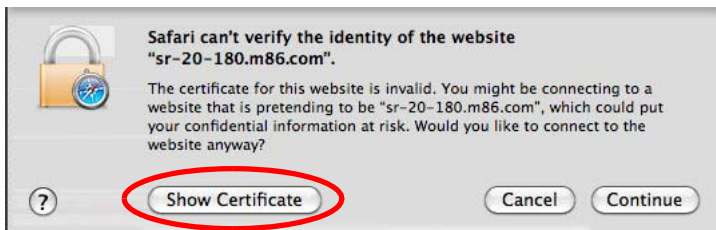
```
hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10      x.acme.com               # x client host
127.0.0.1        localhost
190.160.20.104  WFR.logo.com
```

- C. Enter a line in the hosts file with the WFR's IP address and its host name, and then save and close the file.
- D. In the address field of your newly opened IE browser, from now on you will need to use the WFR's host name instead of its IP address—that is **https://host-name:1443** would be used instead of **https://x.x.x.x:1443**. Click **Go** to open the WFR Welcome window:



## Accept the Security Certificate in Safari

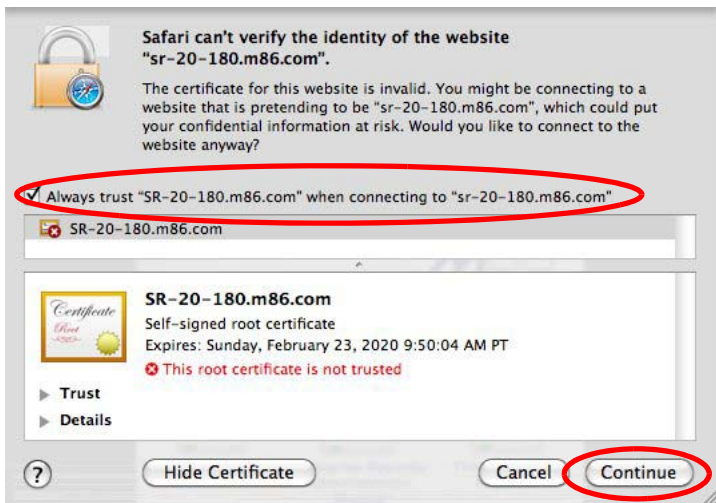
- A. If using a Safari browser, the window explaining "Safari can't verify the identity of the website..." opens:



Click **Show Certificate** to open the certificate information box at the bottom of this window:



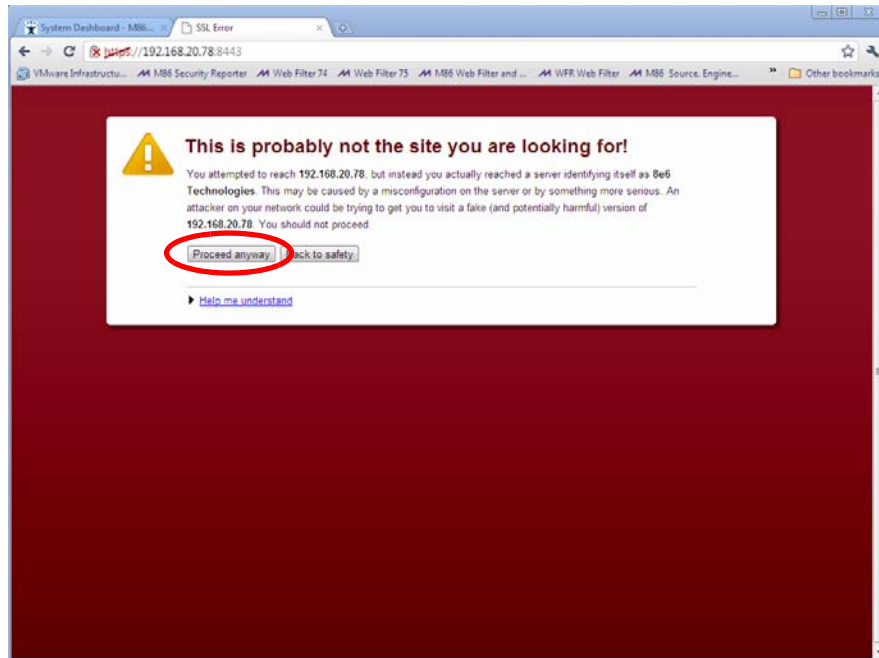
- B. Click the "Always trust..." checkbox and then click **Continue**:



- C. You will be prompted to enter your password in order to install the certificate.

## Accept the Security Certificate in Chrome

If using a Chrome browser, in the page “This is probably not the site you are looking for!” click the button **Proceed anyway**:



Clicking this button launches the WFR Welcome window:



**NOTE:** The Security Certificate must be accepted each time a new browser is launched.