# ACCEPT THE SECURITY CERTIFICATE FOR SR

## Access the SR via its LAN 1 IP Address

A. Launch an Internet supported browser:

- Firefox 6.0
- Internet Explorer 8.0
- Safari 5.1
- Google Chrome 13.0

B. In the address field, type in the LAN 1 IP address you assigned to the SR. Be sure to use "https" and port  **:8443** for a secure connection, appended by "/SR/". For example, if the SR were assigned an IP address of 10.10.10.10, you would enter **https://10.10.10.10:8443/SR/** 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.
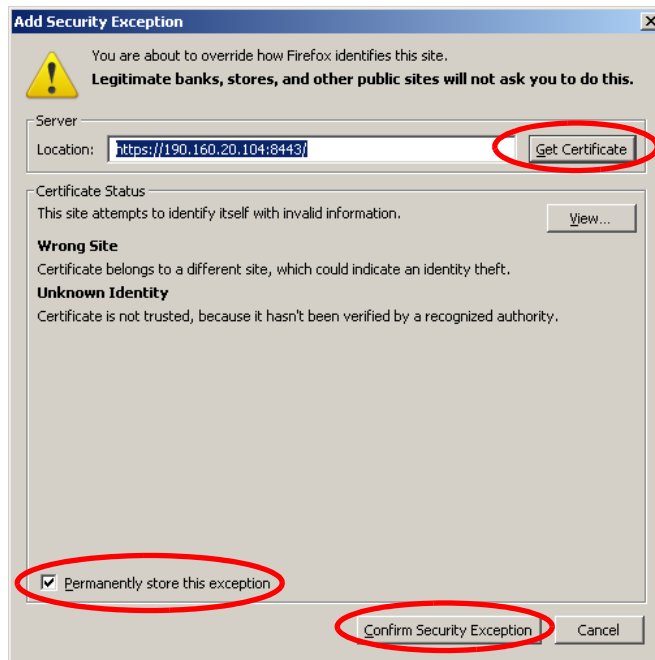
# Accept the Security Certificate in Firefox

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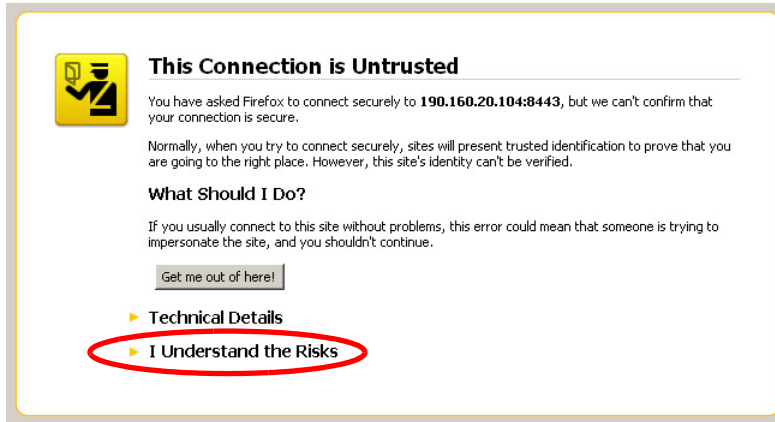


B. In the next set of instructions that display, click **Add Exception...**:
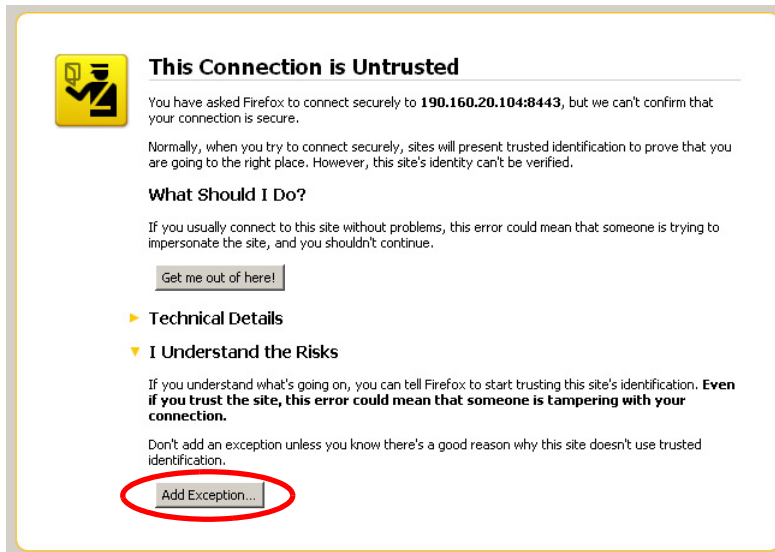


Clicking Add Exception opens the Add Security Exception window:

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 Security Reporter login window:
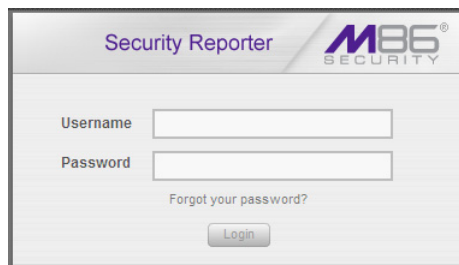


**NOTE**: *On a newly installed unit, SR reporting data will remain inaccessible until logs are transferred to the SR and the database is built.*

# 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
- Windows 7 with IE 8

### Windows XP or Vista with IE 8

A. If using an IE 8 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)**:
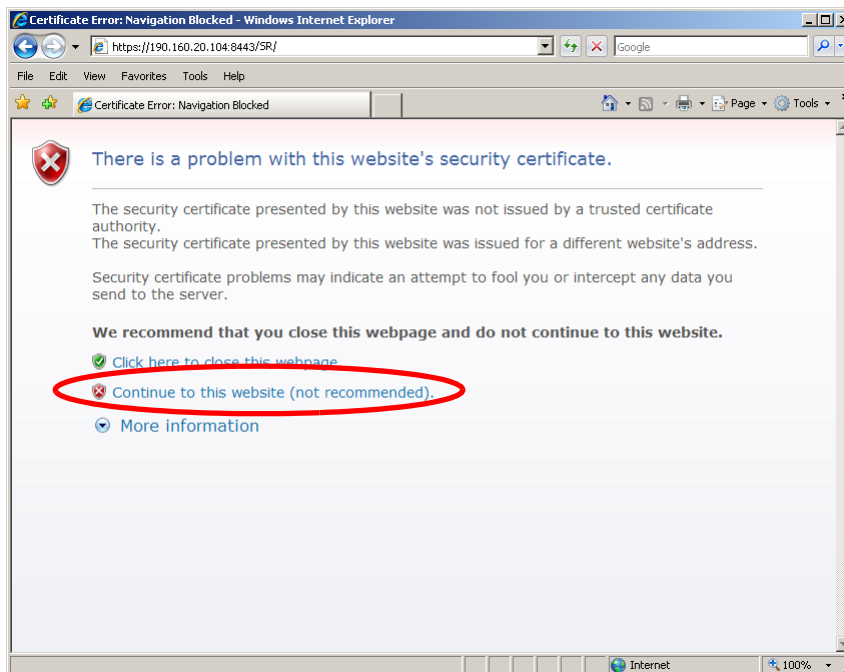


*Figure A1: Windows XP, IE 8*

Selecting this option displays the Security Reporter login window with the address field and the Certificate Error button to the right of the field shaded a reddish color:
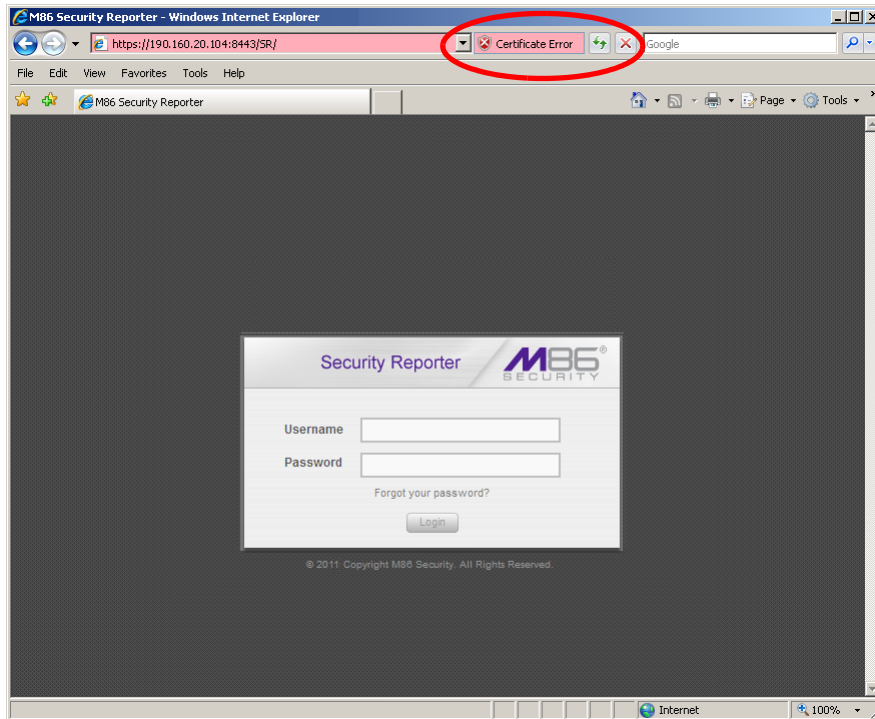
*Figure A2: Windows XP, IE 8*

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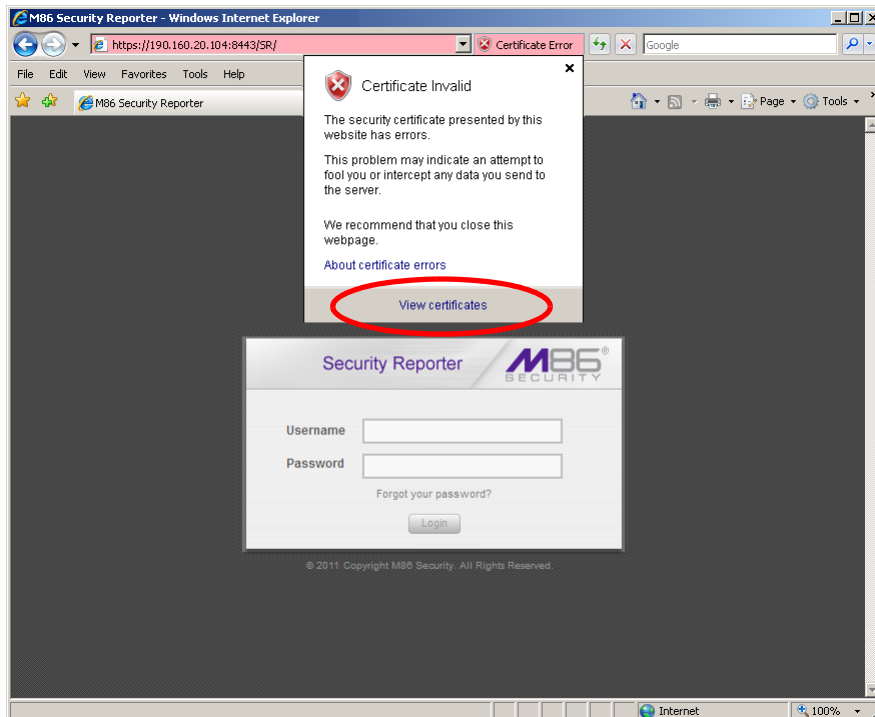


*Figure B: Windows XP, IE 8*

C. Click **View certificates** to open the Certificate window that includes the host-name you assigned to the SR:
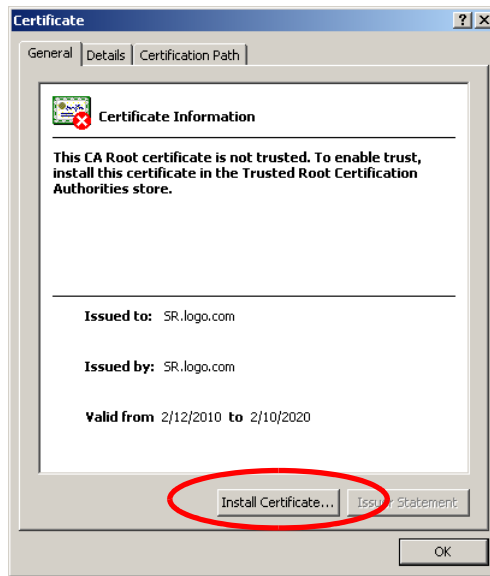
*Figure C: Windows XP, IE 8*

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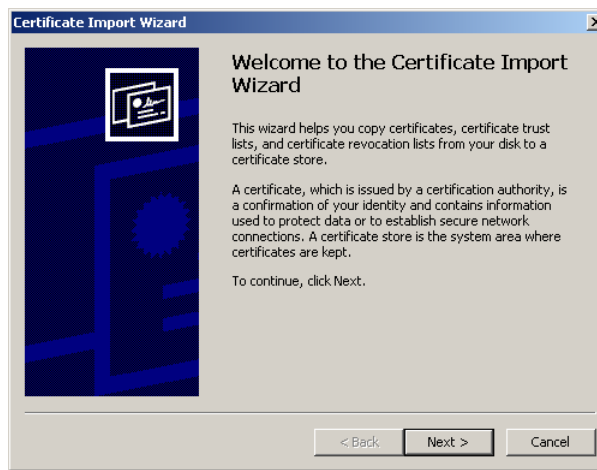


*Figure D: Windows XP, IE 8*

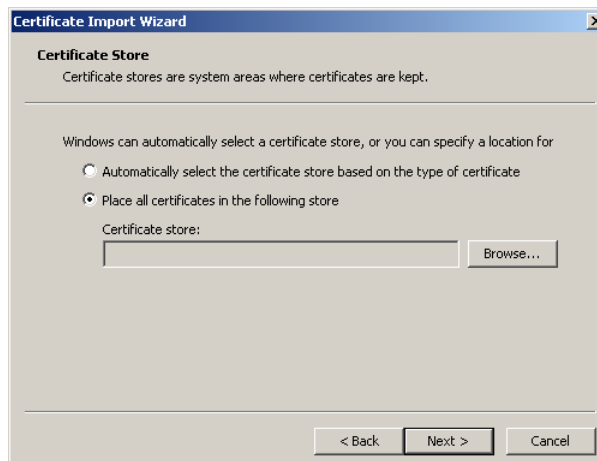E. Click **Next >** to display the Certificate Store page:



*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 pop-up box:



*Figure F: Windows XP, IE 8*

G. Choose "Trusted Root Certification Authorities" and then click **OK** to close the pop-up box.

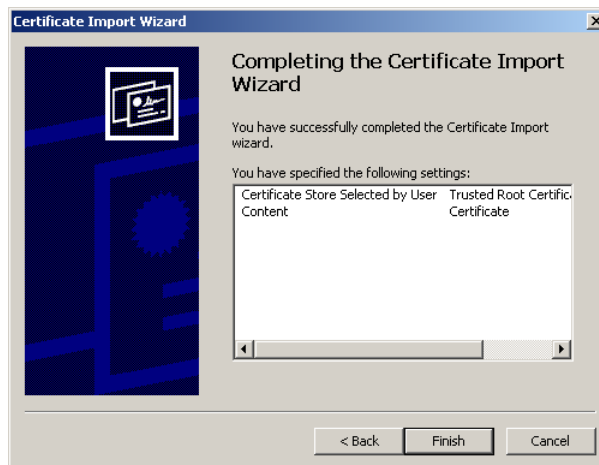H. Click **Next >** to display the last page of the wizard:



*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:
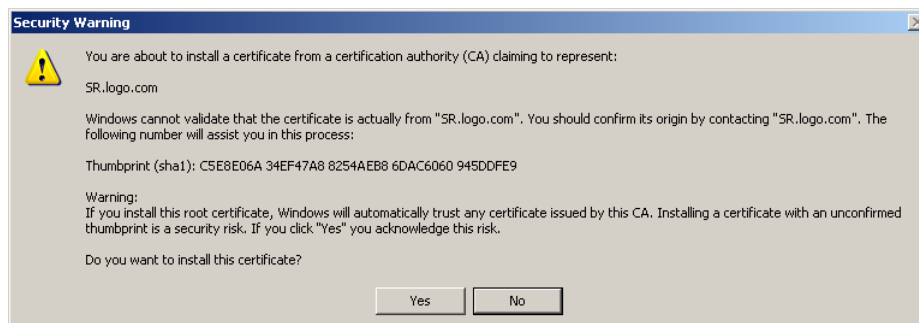


*Figure I: Windows XP, IE 8*

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 SR's IP address to its hostname. Proceed to Map the SR's IP Address to the Server's Hostname.

## Windows 7 with IE 8

A. If using an IE 8 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 pop-up box.

C. Select the Security tab, click **Trusted sites**, and then click **Sites** to open the Trusted sites pop-up box.

D. In the Trusted sites pop-up box, confirm the URL displayed in the field matches the IP address of the SR, and then click **Add** and **Close**.

E. Click **OK** to close the Internet Options pop-up 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:

- 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 Security Reporter login 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 pop-up box (see Figure B).
- Click **View certificates** to open the Certificate window that includes the host-name you assigned to the SR (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 pop-up box (see Figure F).
- Choose "Trusted Root Certification Authorities" and then click **OK** to close the pop-up 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 certif-icate is installed, the alert window opens to inform you the certificate installa-tion 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 pop-up box.

I. Select the Security tab, click **Trusted sites**, and then click **Sites** to open the Trusted sites pop-up box.

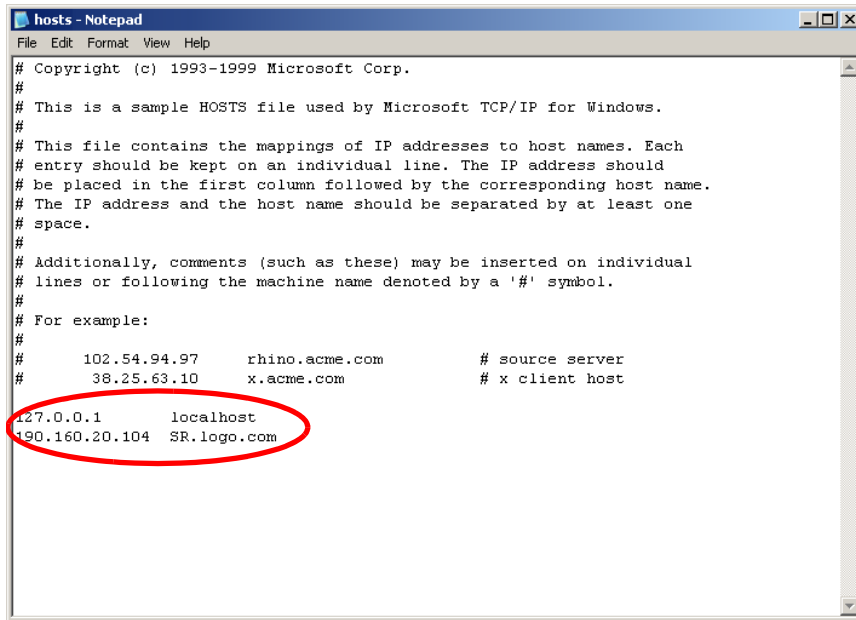J. Select the URL you just added, click **Remove**, and then click **Close**.

Now that the security certificate is installed, you will need to map the SR's IP address to its hostname. Proceed to Map the SR's IP Address to the Server's Hostname.

## *Map the SR's IP Address to the Server's Hostname*

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:
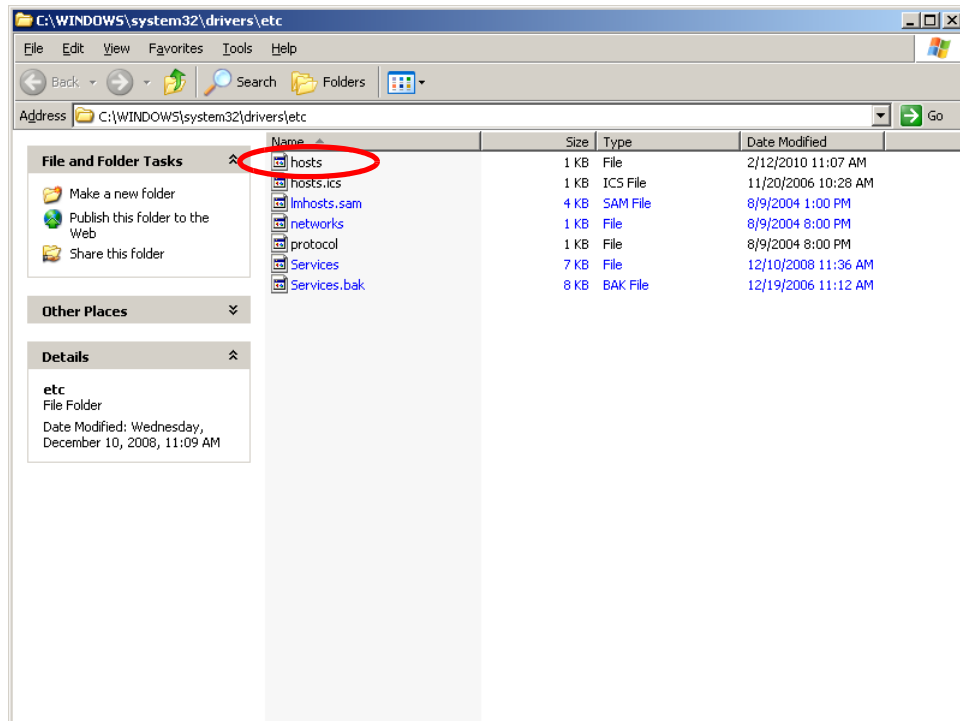


B. Double-click "hosts" to open a window asking which program you wish to use to open the file. Double-click "Notepad" or "TextPad" to launch the hosts file using that selected program:

C. Enter a line in the hosts file with the SR's IP address and its hostname, 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 SR's hostname instead of its IP address—that is **https://host-name:8443/SR/** would be used instead of **https://x.x.x.x:8443/SR/** . Click **Go** to open the Security Reporter login window:
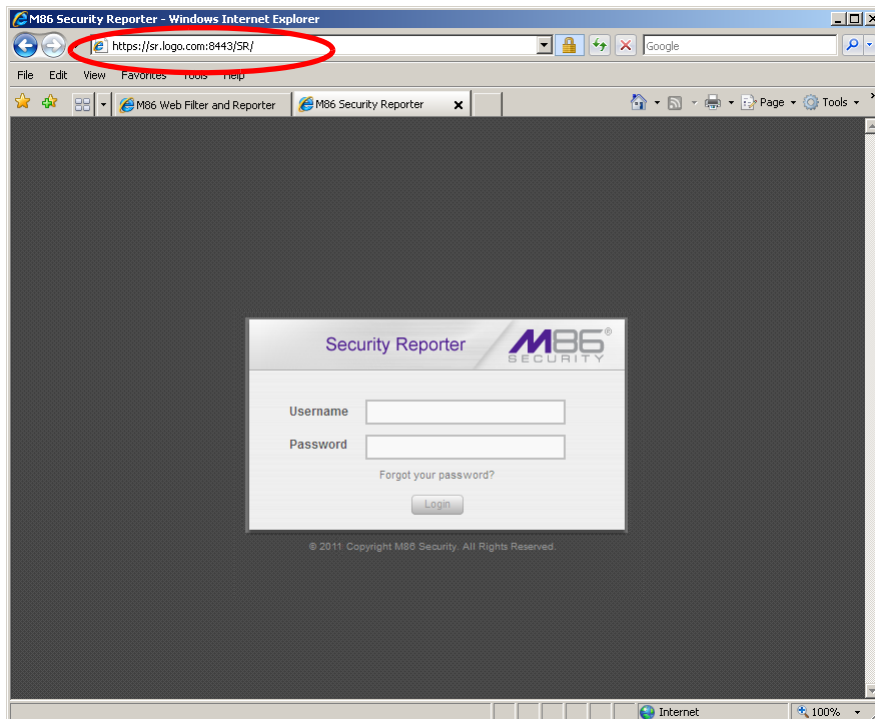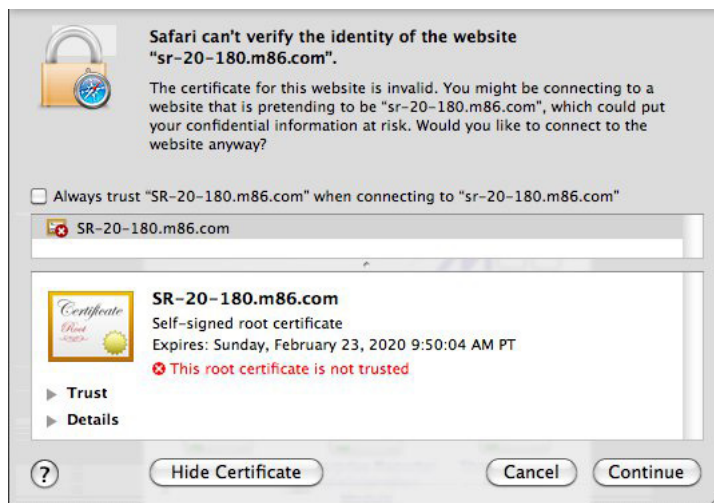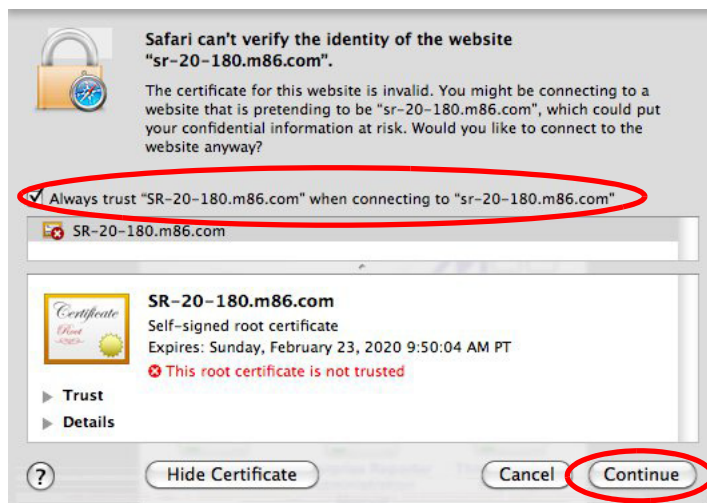
# Accept the Security Certificate in Safari

A. If using a Safari browser, the pop-up window "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.

After the security certificate is installed, the Security Reporter login window displays.

# 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**:
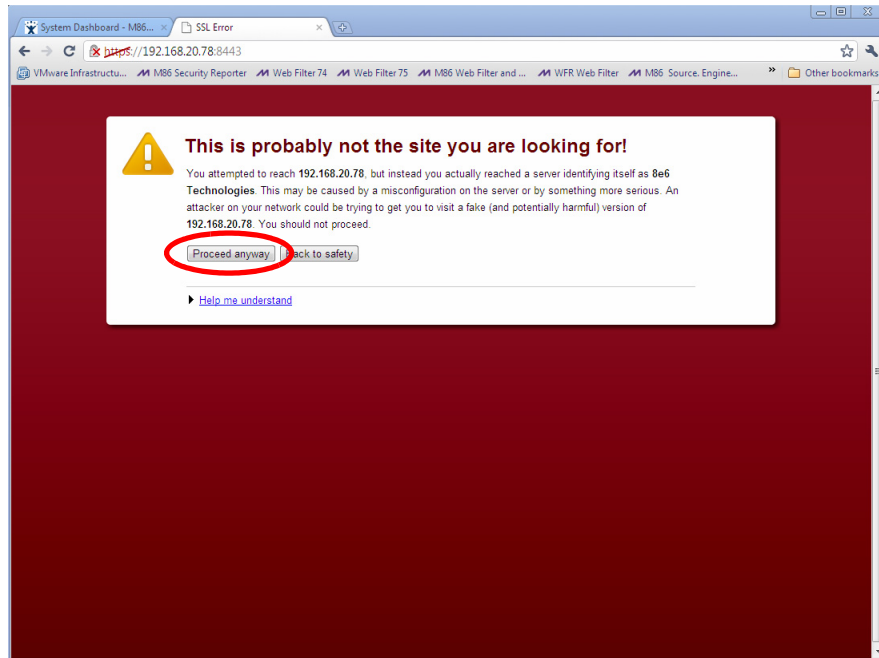


Clicking this button launches the Security Reporter login window:



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