Creating SSL Certificate

for

Midspan Secured Web Server

User Guide

Revision 1.3

Catalog Number 06-0059-056

Contents

1. Introduction 3
2. SSL and Certificates Overview 5
3. Creating Your Own Certificate Authority Files 7
3.1. Creating Your Own Private Certificate Authority 8
3.1.1. Uploading a Private Certificate Authority File to Windows IE7 8
3.1.2. Uploading Private Certificate Authority File to Windows Firefox 3.0.5 10
3.2. Creating the Certificate Files 12
3.3. Uploading a Private Key and Certificate Files to Midspan Secured Web Server 13
3.4. Enabling the Midspan Secure Web SSL 15
4. Obtaining SSL Certificate from Authorized Certificate Authorities 16
4.1. Creating a Secured Web Server Private Key File 17
4.2. Creating the Information Files 18
4.3. Uploading a Trusted Key and Certificate Files to Midspan Secured Web Server 19
4.4. Enabling the Midspan Secure Web SSL 20
5. Appendix A: Evaluating a Thawte Certificate 21
5.1. Creating the Certificate 21
5.2. Uploading the Certificate 23
6. Appendix B: Evaluating a VeriSign Certificate 24
6.1. Creating the Certificate 24
6.2. Uploading the Certificate 25

1 Enterprise, Aliso Viejo, CA 92656, USA; Within the USA: (800) 713-4113, Outside the USA: (949) 221-7100 Fax: (949) 756-0308

1. Introduction

This document describes how to add a valid SSL certificate to the PowerView Pro Secure Web Server (HTTPS). Valid SSL certificate is required to eliminate warning messages (see Figure 1 and Figure 2) displayed by the Web Browser, whenever a remote user attempts to browse to secure Web site lacking valid certificate.

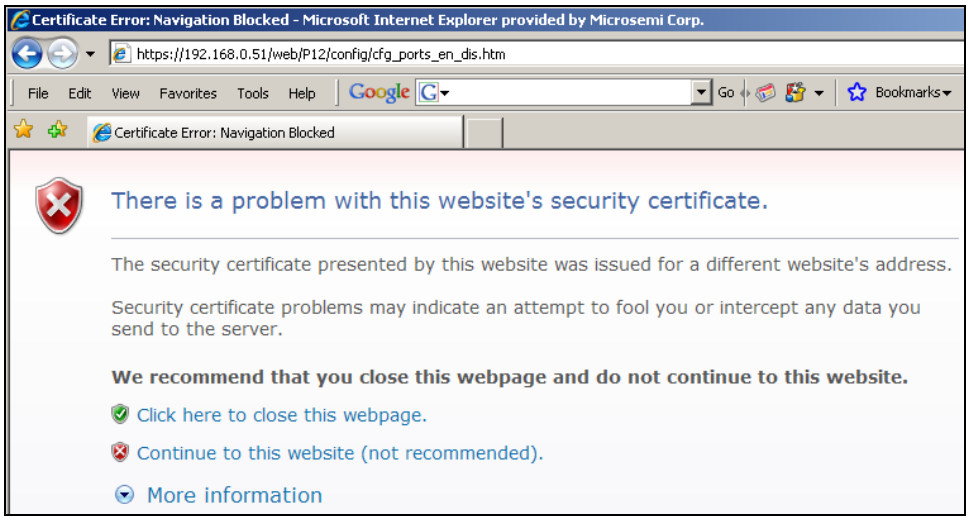


Figure 1: Windows IE7 Warning when Browsing to Non-Trusted Secured Web Site

Figure 2: Mozilla Firefox Warning when Browsing to Non-Trusted Secured Web Site

Two types of solutions are covered by this document:

- Using your own private certificate authority which involves:
  - Creating your own certificate authority files.
  - Creating Midspan secured Web server certificate files (IP address dependent) and uploading them via TFTP to Midspan's secure Web server.
  - Update each Web browser used to browse to Midspan's PowerView Pro GUI using your own private certificate authority files.
- Using trusted certificate authorities such as VeriSign or Thawte:
  - Create a certificate request file and forward it to a recognized certificate authority; for example. VeriSign or Thawte.
  - Pay the required fee to get a valid certificate (IP address) for a limited period of time
  - Upload the received certificate to Midspan's embedded Web server

NOTE:

To purchase an official certificate from VeriSign or Thawte, you first need to purchase a valid DNS name for each Midspan IP address.

Certificate creation requires opening the www.openssl.org free open source application. **openssl.exe,** and **openssl.cnf** files are required for this process (included on CD). For your convenience, several batch files were added to ease the certificate creation process.

After becoming familiar with the certificate creation process, you may modify the batch files according to your specific needs (for example, change created certificate file names, certificate expiration date, etc.).

2. SSL and Certificates Overview

When browsing to https://www.amazon.com (see Figure 3), a secured SSL connection is established as Amazon purchased a certificate from VeriSign. All Web browsers such as Windows IE6/IE7, Firefox2/3 already include VeriSign, as a trusted certificate authority.

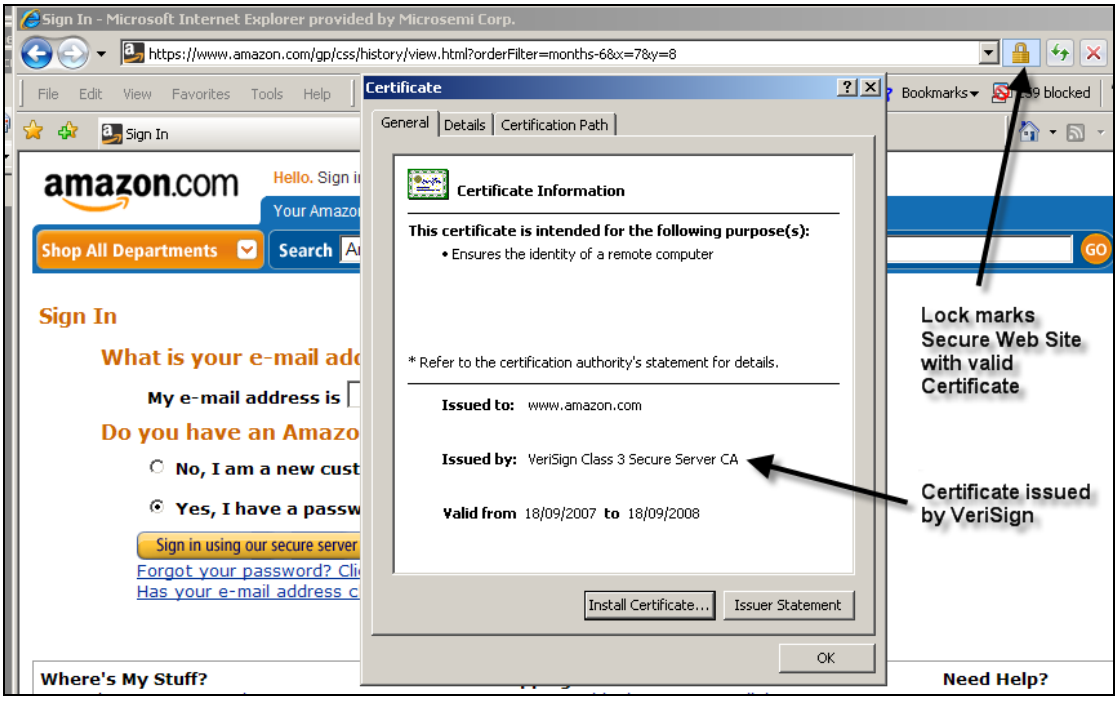


Figure 3: www.amazon.com Certificate Information

When a Web browser client connects to a secured Web server, the server sends a certificate to the client. This certificate has three major elements:

- Name (that is the server's address, for example www.amazon.com)
- Public key such as RSA 512 bits
- Signature (by a trusted third party such as VeriSign, that vouches for the name and the public key)

NOTE:

Each SSL Web server must have a unique certificate. You cannot reuse an SSL server certificate. The certificates are distinguished by the "common name" or "CN" marked on the certificate.

When a Web browser is installed on your PC, it comes with a list of trusted certificate authorities (see Figure 4 and Figure 5) such as VeriSign, Thawte, etc.

1 Enterprise, Aliso Viejo, CA 92656, USA; Within the USA: (800) 713-4113, Outside the USA: (949) 221-7100 Fax: (949) 756-0308

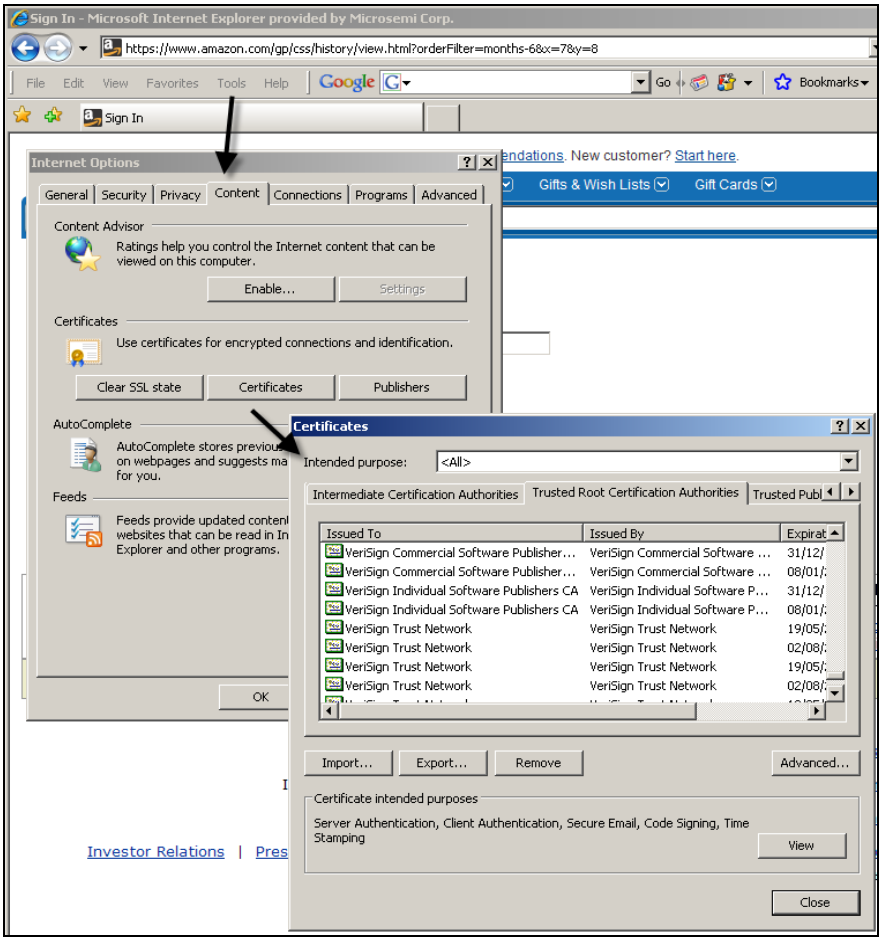


Figure 4: List of Preinstalled Trusted Authorities in Windows IE7

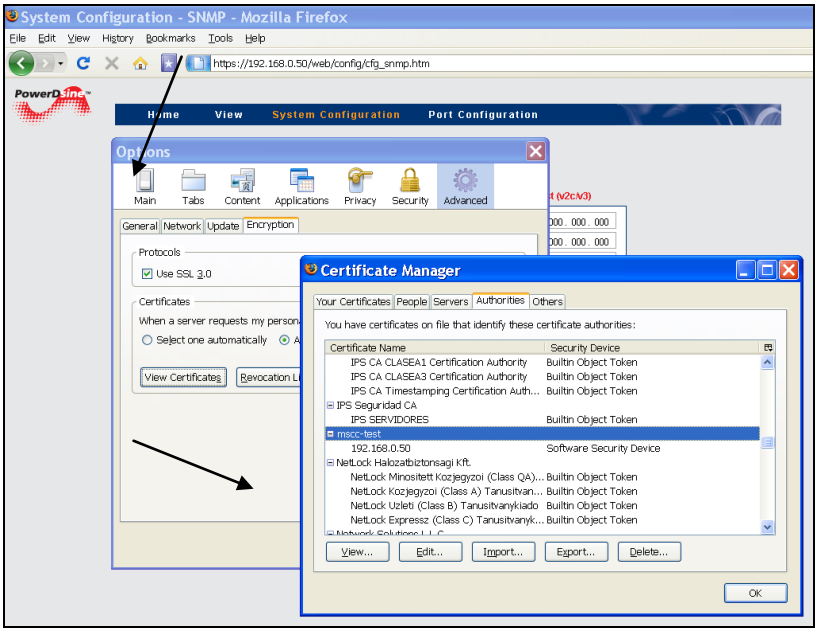


Figure 5: List of Preinstalled Trusted Authorities in Mozilla Firefox 3.0.5

3. Creating Your Own Certificate Authority Files

This section details the procedure for creating your own certificate authority files; Figure 6 illustrates the required flow.

The procedure consists of the following steps:

- Creating Your Own Private Certificate Authority, page 8
- Creating the Certificate Files, page 12
- Uploading a Private Key and Certificate Files to Midspan Secured Web Server, page 13
- Enabling the Midspan Secure Web SSL, page 15

Use the following flow chart to determine which steps are needed for your particular setup.

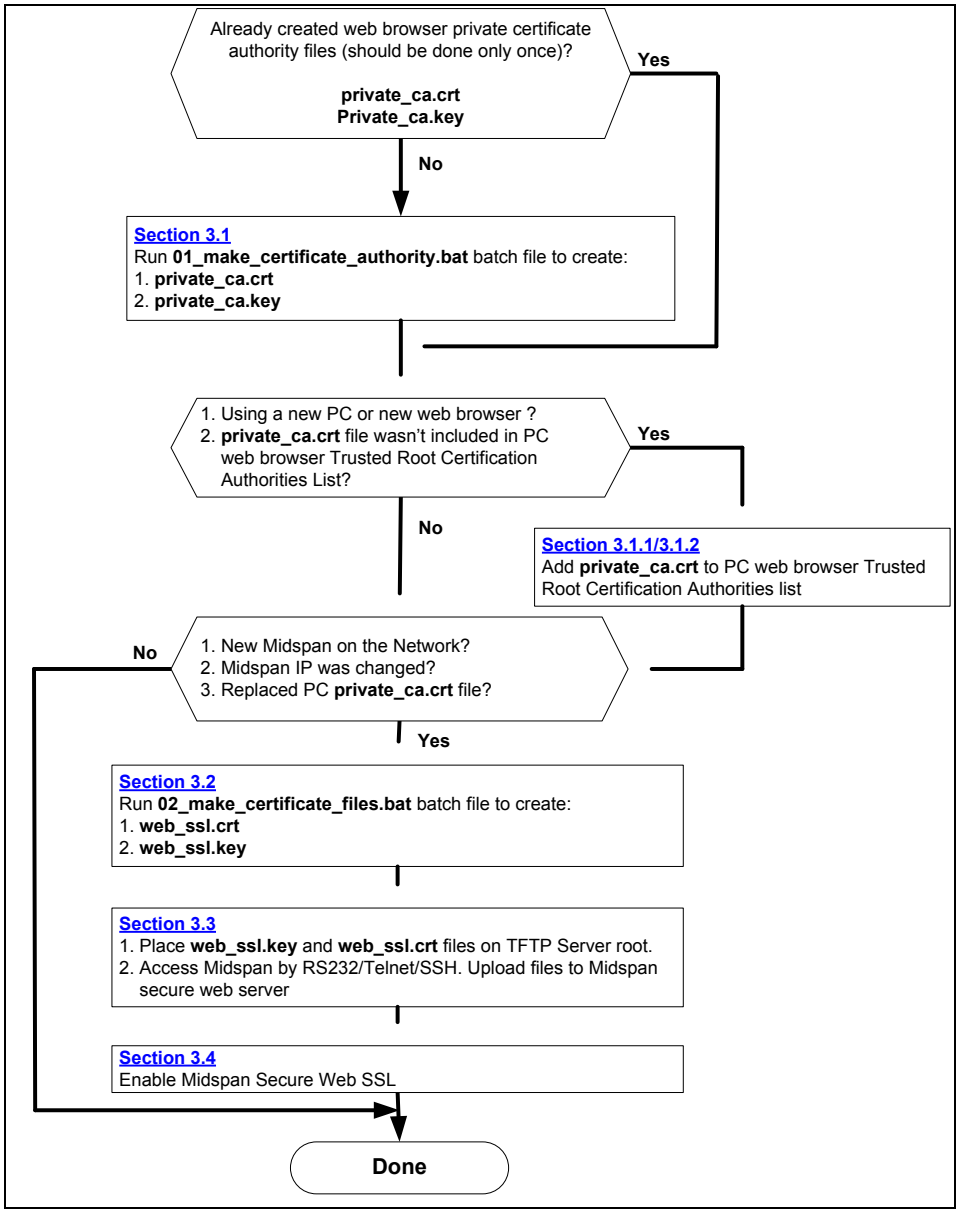


Figure 6: Using Your Own Private Certificate Authority Process

3.1. Creating Your Own Private Certificate Authority

The following procedure describes how to create the private certificate authority. The private certificate file is used as authentication when browsing to a Midspan PowerView Pro secured Web server.

1. On the provided CD, browse to *Use your own private Certificate Authority* folder.
2. Run **01_make_certificate_authority.bat**. This file contains the following text:
   - set OPENSSL_CONF=openssl.cnf
   - openssl genrsa -out private_ca.key
   - openssl req -new -key private_ca.key -x509 -days 3650 -out private_ca.crt
3. Enter the following information:

Country Name (two letter code) [AU]		**US**
State or Province Name (full name) [Some-State]		**MyState**
Locality Name (e.g., city) []		**MyCity**
Organization Name (e.g., company) [Internet Widgits Pty Ltd]	:	**MyCompany**
Organizational Unit Name (e.g., section) []		**MybusinessDivision**
Common Name (e.g., YOUR name) []		**MyCompany MyState**
Email Address []		xxx

Two files are created:

- **private_ca.key**: Contains certificate authority private key used later to create Midspan certificate files
- **private_ca.crt:** Certificate file should be **uploaded to each computer** (see procedure below, Section 3.2.1 and Section 3.2.2).

private_ca.crt provides authentication when browsing to a Midspan PowerView Pro secured Web server.

NOTE:

Batch file *01_make_certificate_authority.bat* should be executed only once.

3.1.1. Uploading a Private Certificate Authority File to Windows IE7

The following procedure describes how to upload the *private_ca.crt* file to Windows IE7 Web Browser. This procedure must be repeated for each computer used to browse to Midspan Secured Web Server.

1. Select:

   Tools -> Internet Options -> Content -> Certificates -> Trusted Root Certificate Authorities

   (Figure 7, Figure 8, and Figure 9.)

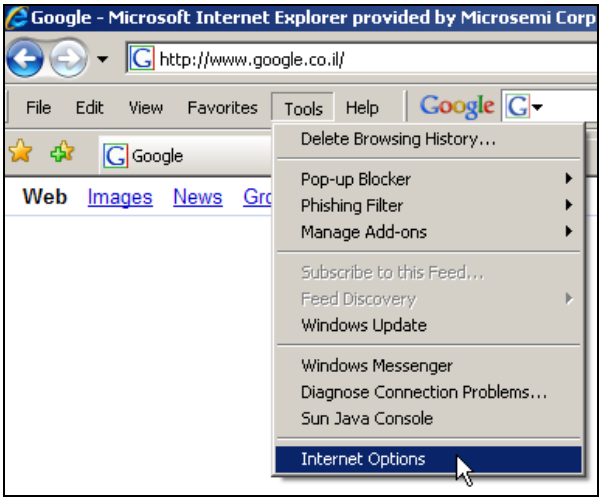


Figure 7: Tools > Internet Options

Figure 8: Internet Options > Content > Certificates

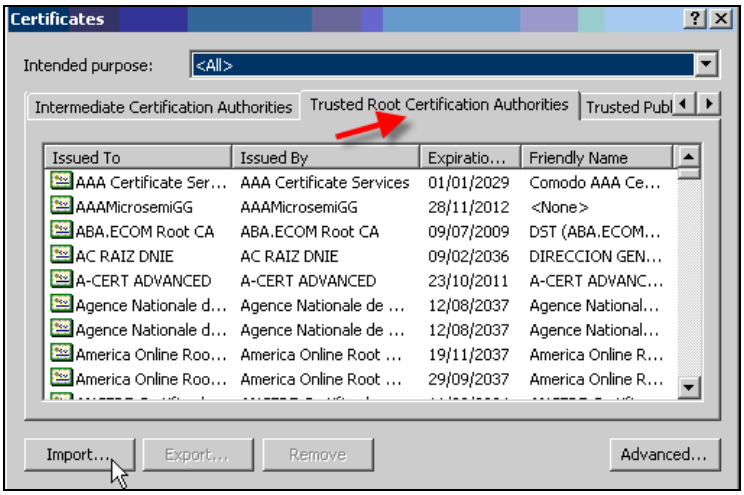


Figure 9: Trusted Root Certificate Authorities

2. Click **Import**.

   The **Certificate Import Wizard** appears (Figure 10).

Figure 10: Certificate Import Wizard

3. Click **Next**.
4. Browse to the folder where you created **private_ca.crt**.

5. Select the file.
6. Click **Next**.
7. Click **Finish**.
8. Click **End**.

   The new added certificate authority's file is displayed as typed in the "Common Name" field (MyCompany MyState in Figure 9).

3.1.2. Uploading Private Certificate Authority File to Windows Firefox 3.0.5

The following procedure describes how to upload the private_ca.crt file to Windows Firefox Browser. This procedure must be repeated for each computer used to browse to Midspan Secured Web Server.

1. On the menu baron the top section select:

   Tools-> Options -> Advanced -> Encryption -> View Certificates

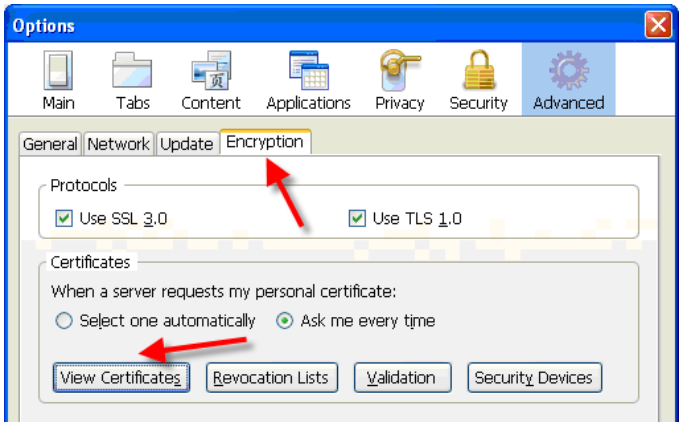


Figure 11: Tools-> Options -> Advanced -> Encryption -> View Certificates

   The Manage Certificates window appears.

2. Click **Authorities Tab**.

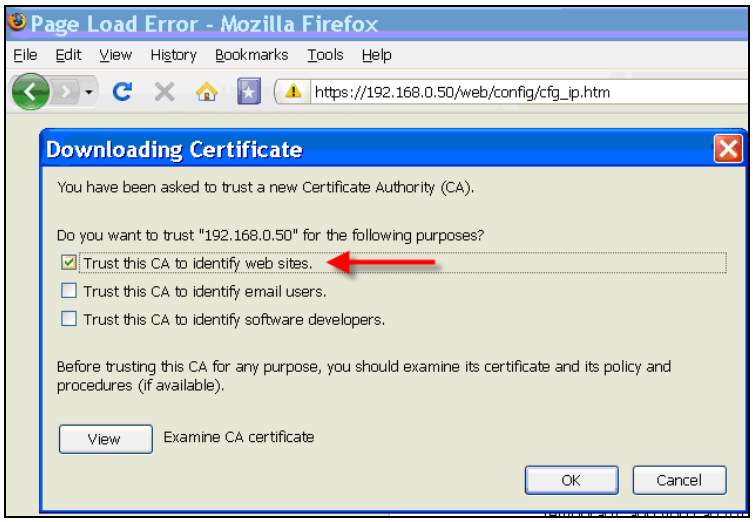


Figure 12: Authorities Tab

3. Mark the **Trust this CA to identify web sites** box.
4. Click **OK**.
5. Scroll down the certificate name list; when the desired certificate name appears (for example *webmail.umac*.mo) under the *University of Macau*, it means that the appropriate certificate is installed.

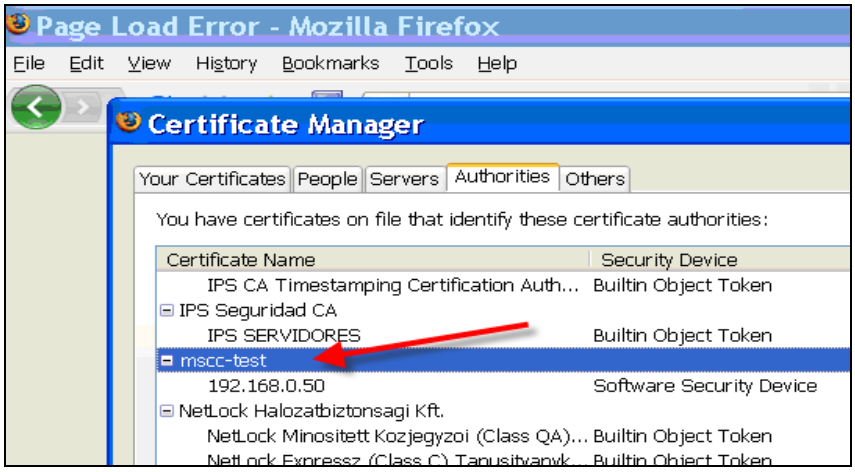


Figure 13: Certificate Manager Example

6. Click **OK**.

   All windows close.

3.2. Creating the Certificate Files

The following procedure describes how to create certificate files. The files created are uploaded to the Midspan or used to obtain a certificate from certified Certificate Authorities.

1. Run **02_make_certificate_files.bat**, which contains the following text:
   - set OPENSSL_CONF=openssl.cnf
   - openssl genrsa -out web_ssl.key
   - openssl req -new -key web_ssl.key -out web_ssl.csr
   - openssl x509 -req -days 365 -in web_ssl.csr -CA private_ca.crt –Cakey
   - private_ca.key -CAcreateserial -out web_ssl.crt
2. Enter the following information:

Country Name (two letter code) [AU]		**US**
State or Province Name (full name) [Some-State]		**MyState**
Locality Name (e.g., city) []		**MyCity**
Organization Name (e.g., company) [Internet Widgits Pty Ltd]	:	**MyOrganization**
Organizational Unit Name (e.g., section) []		**MyUnit**
Common Name (e.g., YOUR name) []		**192.168.0.50**
Email Address []		

Must match Midspan IP Address

3. Enter the following 'extra' attributes to be sent with your certificate request:
   - A challenge password []
   - An optional company name []

Four files are created:

- **private_ca.srl**
- **web_ssl.key** – Contains Midspan secured Web server private key. This file must be uploaded to a Midspan with the same IP address (see procedure below – Section 3.4) as typed when the ***02_make_certificate_files.bat*** batch file was executed.
- **web_ssl.csr** – Contains Midspan secured Web server certificate request. This file is equivalent to the certificate request file being generated by Microsoft IIS Web Server/Apache Web Server.

NOTE:

This file is utilized to obtain a certificate from certified Certificate Authorities such as VeriSign, Thawte (see below; how to obtain certificate from authorized certificate authorities).

- **web_ssl.crt** – Contains Midspan secured Web server certificate. This file (together with web_ssl.key) must be **uploaded** to a Midspan with the same IP address (see Section 3.4, as entered when the ***02_make_certificate_files.bat*** batch file was executed.

NOTE:

Batch file *02_make_certificate_files.bat* **must be executed for each Midspan being installed on the Network. Midspan's IP address** must **match the IP address as typed when the 2nd batch file was executed.**

3.3. Uploading a Private Key and Certificate Files to Midspan Secured Web Server

The following procedure describes how to upload the private key ***web_ssl.key*** file and certificate ***web_ssl.crt*** file to the Midspan secured Web server.

1. Run TFTP Server.

   The NBTFTP Server window appears (Figure 14).

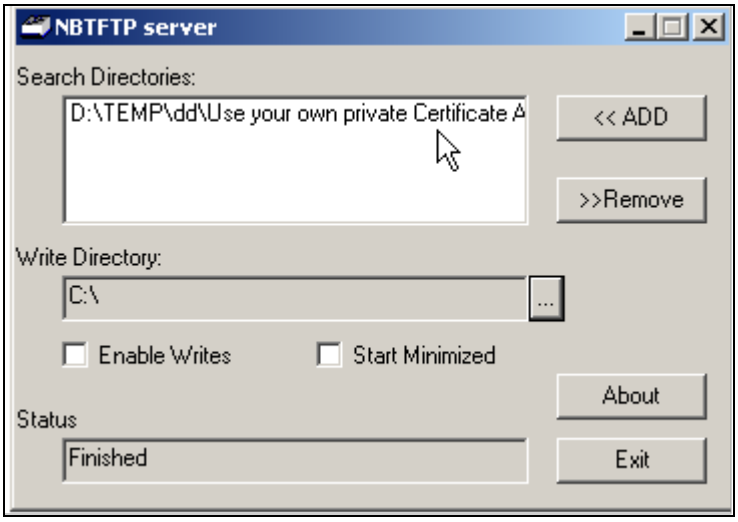


Figure 14: NBTFTP Server

2. Click **Add**.

3. Browse to the required directory and add a folder containing the ***web_ssl.key*** and ***web_ssl.crt*** to the TFTP Server root path.

4. Click **Exit**.

5. Via RS232 or Telnet, connect to the Midspan (Telnet default administrator user name is ***admin*** and the password is "***password***").

6. Click **Esc**.

7. Select **Configuration & maintenance** menu.

8. Download the **Web SSL Certificate**. Figure 15 illustrates the process.

   a. Type "Y" when requested to download the Web SSL certificate to Midspan.
   b. Type "Y" when requested to verify that you have a Private Key & Certificate Files
   c. Enter the TFTP Server IP address.
   d. Enter the private key file name: ***web_ssl.key***
   e. Enter the certificate file name: ***web_ssl.crt***

```
Download WEB SSL certificate from TFTP Server - are you sure (Y/N,ESC) ?
Verify that Private-Key & Certificate files are on TFTP Server - (Y/N,ESC) ?

Enter remote TFTP Server IP address :192.168.0.40

Enter WEB SSL Private-Key file name (for example web_ssl.key):web_ssl.key
TFTP start...Received 493 bytes

Enter WEB SSL Certificate file name (for example web_ssl.crt):web_ssl.crt
TFTP start....Received 713 bytes

Manager module will be RESET in 1 Sec !!
```

Figure 15: Download Instructions

Upon successful downloading of the ***web_ssl.key*** and ***web_ssl.crt*** files, the Midspan Network Management module resets itself without affecting the operational PoE ports.

9. Close and reopen your Web browser.

1 Enterprise, Aliso Viejo, CA 92656, USA; Within the USA: (800) 713-4113, Outside the USA: (949) 221-7100 Fax: (949) 756-0308

3.4. Enabling the Midspan Secure Web SSL

1. Browse to Midspan IP address (for example 192.168.0.50).
2. From the **System Configuration** menu, select **Security** (Figure 16).

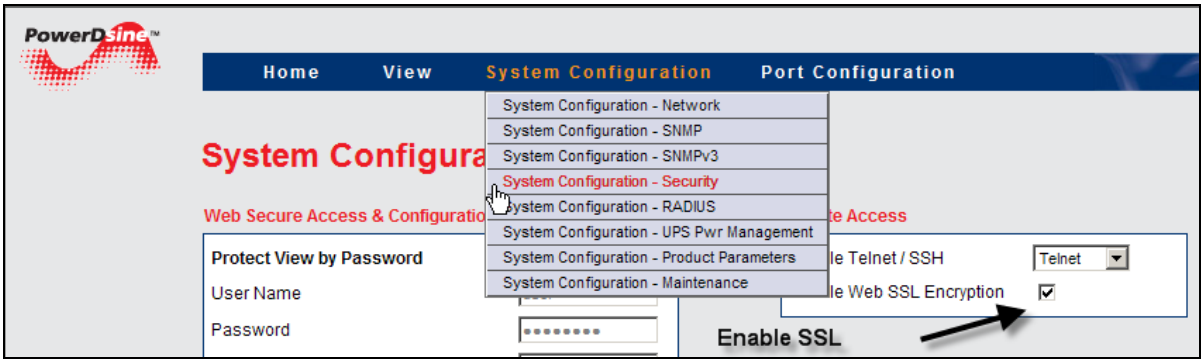


Figure 16: Enabling SSL

3. Mark the **Enable SSL** checkbox.
4. Click **Update**.
5. Click **Save**.
6. Close and reopen your Web browser. Note that *https* appears in the URL address field and the *lock symbol* is depressed (Figure 17).

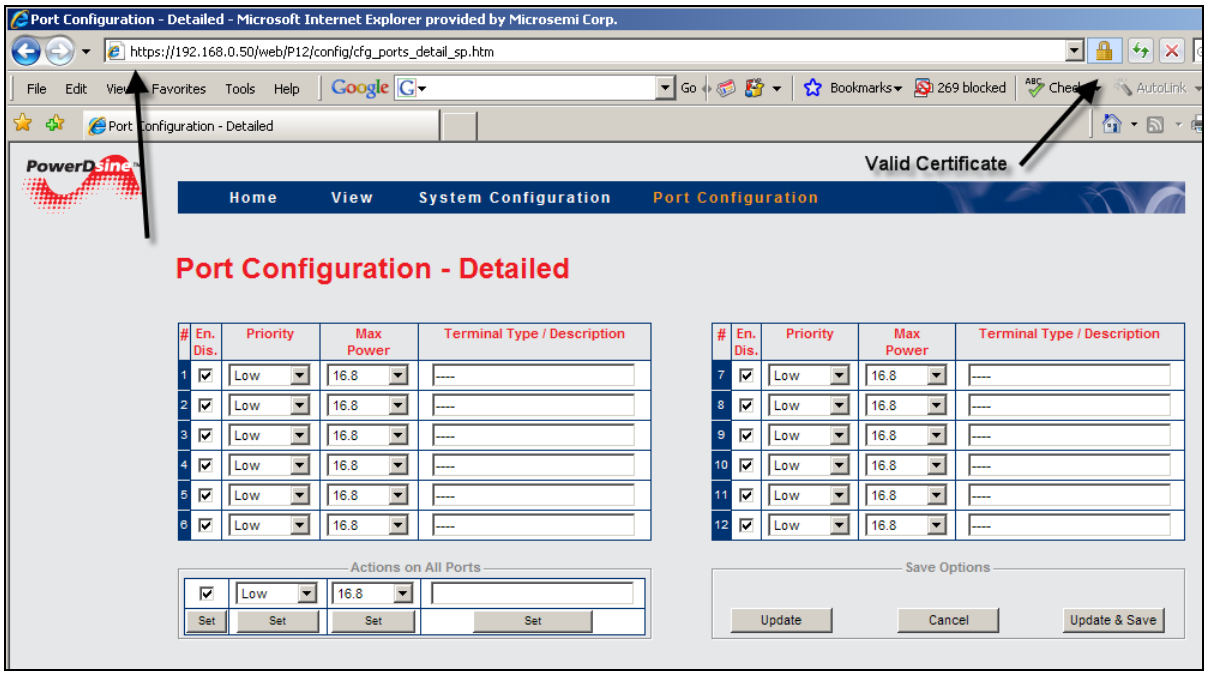


Figure 17: Port Configuration – Detailed Window

NOTES:

All Midspan's Web pages beside the main Web page and View-Status Web pages will be SSL encrypted.

View-Status Web page isn't encrypted, as it combines many images that slow down the Web page display over the SSL connection.

4. Obtaining SSL Certificate from Authorized Certificate Authorities

This section details how to obtain certificate authority files from authorized sources. The procedure consists of the following steps:

- Creating a Secured Web Server Private Key File, page 17
- Creating the Information Files, page 18
- Uploading a Trusted Key and Certificate Files to Midspan Secured Web Server, page 19
- Enabling the Midspan Secure Web SSL, page 20

Figure 18 describes the flow required to obtain SSL Certificate from an authorized certificate authorities such as Verisign, Thawte and Updating Midspan Secured Web Server. Use the chart to determine which steps are needed for your particular setup.

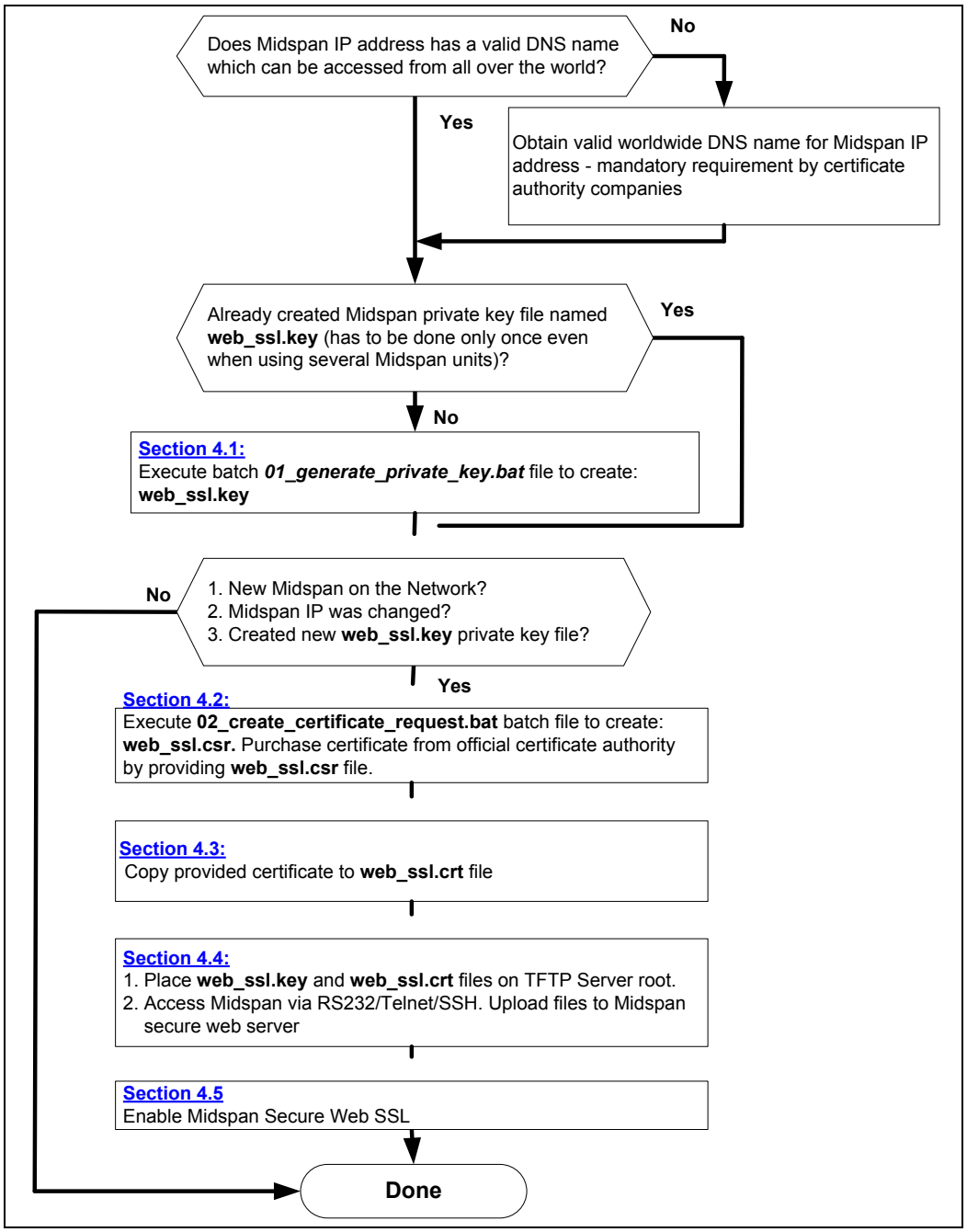


Figure 18: Obtaining a SSL Certificate from Authorized Certificate Authorities Process

4.1. Creating a Secured Web Server Private Key File

The following procedure describes how to create a secured web server private key file. This file is to allow other Midspan devices to be added to the network.

1. Switch to **Use official Certificate Authority** folder.
2. Run the **01_generate_private_key.bat** batch file containing the following:
   - **set OPENSSL_CONF=openssl.cnf**
   - **openssl genrsa -out web_ssl.key**

The batch file creates a secured Web server private key file, **web_ssl.key**.

NOTE:

The Web_ssl.key file must be created only once. Save the created web_ssl.key file for later use in cases where another Midspan is added to your network, or the Midspan IP address should be changed.

4.2. Creating the Information Files

The following procedure describes how to create the files containing the relevant information required for the certificate procedure. The files created are used when purchasing a valid certificate from the certificate authority company.

1. Run the **02_create_certificate_request.bat** batch file containing the following:
   - set OPENSSL_CONF=openssl.cnf
   - openssl req -new -key web_ssl.key -out web_ssl.csr
2. Enter the following information:

Country Name (two letter code) [AU] :	US
State or Province Name (full name) [Some-State] :	MyState
Locality Name (for example, a city) []	MyCity
Organization Name (for example, company) [Internet Widgits Pty Ltd]	MyOrganization
Organizational Unit Name (for example, section) []	:MyUnit
Common Name (for example, YOUR name) []	www.MyMidspan.com
Email Address [	

3. Enter the following 'extra' attributes to be sent with your certificate request:
   - A challenge password []
   - An optional company name []

One of the files created is the **web_ssl.csr**: This file is equivalent to the certificate request file generated by Microsoft IIS Web Server/Apache Web Server.

4. Approach your preferred certificate authority company. Provide them with the **web_ssl.csr** file and purchase a valid certificate. Save the purchased certificate as **web_ssl.crt**.

4.3. Uploading a Trusted Key and Certificate Files to Midspan Secured Web Server

The following procedure describes how upload the Trusted Key and Certificate Files to Midspan Secured Web Server.

1. Upload the **web_ssl.key** (created in Section 4.1) and certificate **web_ssl.crt** (created in Section 4.2) files to the Midspan secure web server.
2. Run the **TFTP Server** (Figure 19).

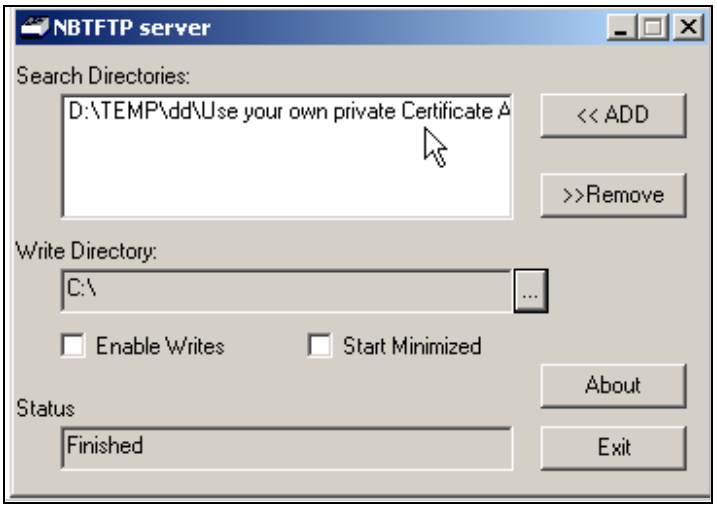


Figure 19: NBTFTP Server Window Dialog Box

3. Add a folder containing the ***web_ssl.key*** and **web_*ssl.crt*** to the TFTP Server root path.
4. Via RS232 or Telnet, connect to the Midspan (Telnet default administrator user name is ***admin*** and password is ***"password"***).
5. Click **Esc**.
6. Select **Configuration & maintenance**.
7. Download the **WEB SSL Certificate**.

```
Download WEB SSL certificate from TFTP Server - are you sure (Y/N,ESC) ?
Verify that Private-Key & Certificate files are on TFTP Server - (Y/N,ESC) ?


Enter remote TFTP Server IP address :192.168.0.40

Enter WEB SSL Private-Key file name (for example web_ssl.key):web_ssl.key
TFTP start...Received 493 bytes


Enter WEB SSL Certificate file name (for example web_ssl.crt):web_ssl.crt
TFTP start....Received 713 bytes

Manager module will be RESET in 1 Sec !!
```

   a. Type "Y" when requested to download the Web SSL certificate to Midspan.
   b. Type "Y" when requested to verify that you have a Private Key & Certificate Files
   c. Enter the TFTP Server IP address.
   d. Enter the private key file name: web_ssl.key
   e. Enter the certificate file name: ***web_ssl.crt***

   After successful downloading of both the Web_ssl.key and the Web_ssl.crt files, the Midspan Network Management module resets itself without affecting the operational PoE ports.

8. Close and reopen your Web browser.

4.4. Enabling the Midspan Secure Web SSL

The following procedure describes how to place key files on the TFTP server and then upload them to the Midspan secure web server.

1. Browse to Midspan using its DNS name or IP address (for example 192.168.0.50).
2. From the **System Configuration** menu, select **Security**.
3. Enable **SSL**.
4. Click **Update & Save**.
5. Close and reopen the Web browser using the **DNS name only**. *Https* appears in the URL field and the *lock symbol* is depressed.

Note: Do use the IP address, as the SSL certificate from an authorized certificate authorities is provided only for DNS name and not specifically for IP address. Browsing via a specific IP address is valid only for trial versions).

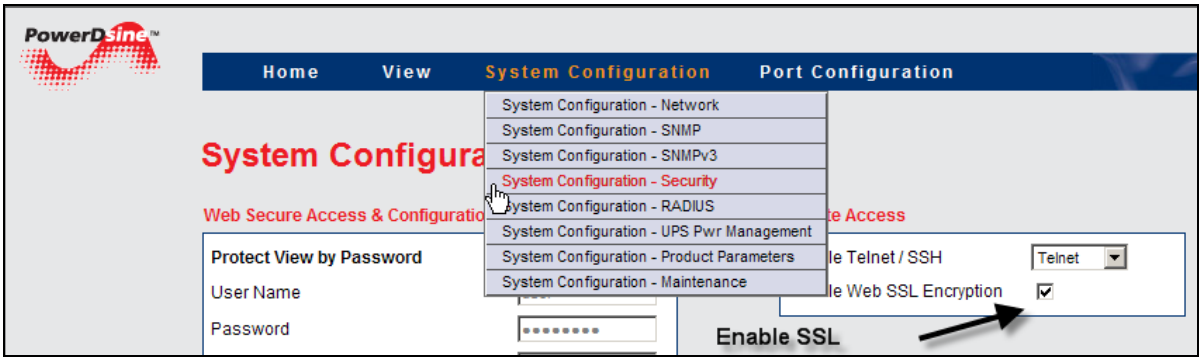


Figure 20: Enabling the SSL

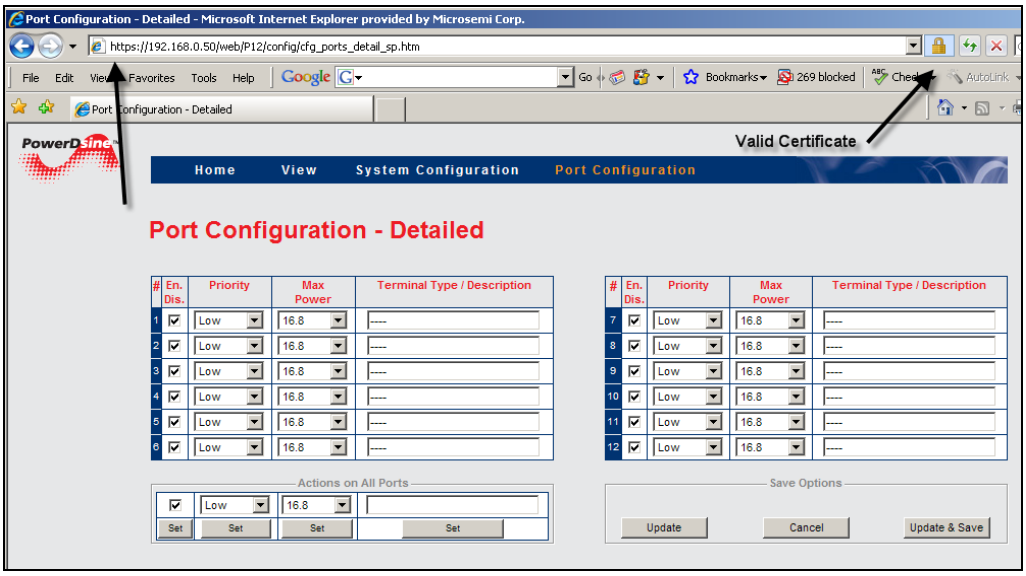


Figure 21: Port Configuration Window Showing Secure Browsing

NOTE:

All Midspan Web pages besides the main Web page and View-Status Web page will be SSL encrypted. View Status Web page isn't encrypted, as it combines many images that slow down the Web page display over the SSL connection.

5. Appendix A: Evaluating a Thawte Certificate

Thawte offers an option to obtain a free SSL trial certificate which is good for 21 days. The following procedure describes how to download and install this certificate.

5.1. Creating the Certificate

1. Execute **01_generate_private_key.bat**.

   The **web_ssl.key** private key is created.

2. Execute **02_create_certificate_request.bat**.

3. Enter the following information:

Country Name (2 letter code) [AU] :	**US**
State or Province Name (full name) [Some-State] :	**MyState**
Locality Name (e.g., city) [] :	**MyCity**
Organization Name (for example company) [Internet Widgits Pty Ltd]:	**MyOrganization**
Organizational Unit Name (for example, section) []:	**MyUnit**
Common Name (for example **YOUR** name) []:	**192.168.0.50**
Email Address []:	
Enter the following 'extra' attributes to be sent with your certificate request	
A challenge password []:	
An optional company name []	

Must match Midspan IP Address

   The **web_ssl.csr** file is created.

4. Browse to https://www.thawte.com/cgi/server/try.exe.

   The web page shown in Figure 22 appears.

5. Select the **SSL 123 Certificate** radio box.

6. Open the **web_ssl.csr** file in Notebook.

7. Copy the file contents.

8. In the text box, paste the file.

9. Click **Next**.

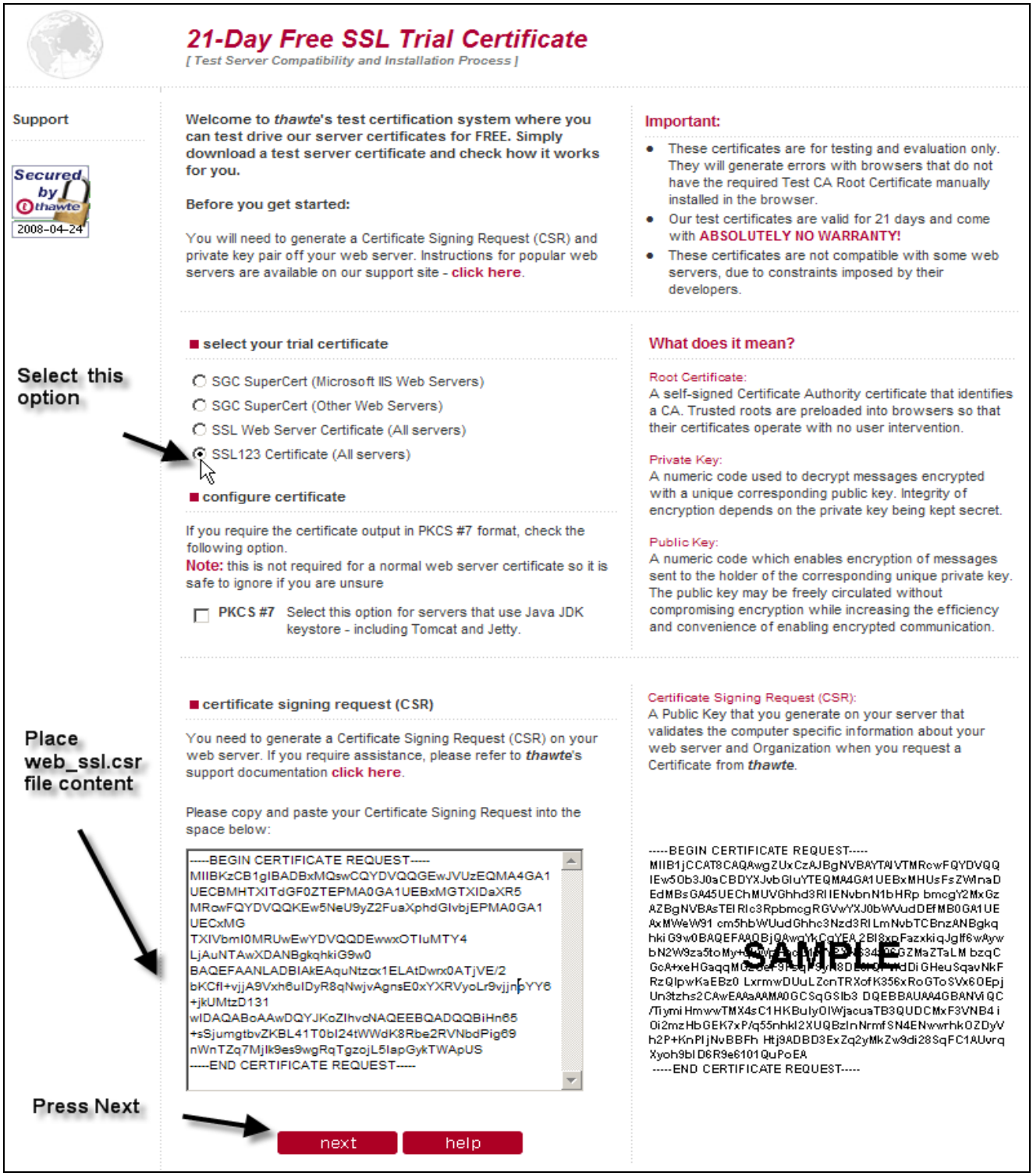


Figure 22: Setting Up the Trial Certificate

10. Create a file named **web_ssl.crt.**

11. Copy the created certificate text and paste the text into web_ssl.crt**.**

The certificate you had received is signed by Thawte certificate authority. However the certificate still has to be installed on your Web browser (evaluation version).

5.2. Uploading the Certificate

1. From: https://www.thawte.com/roots/ download **thawte-roots.zip** (this is the Thawte Test CA Root Certificate).

2. Unzip the file and locate the ***Thawte Test Roots\Thawte Test Root.cer*** file.

3. Open Internet Explorer 7 (or any other browser).

4. Add the certificate to the Trusted Root Certification Authorities list by performing the following (detailed in Sections 3.1.1 and 3.1.2):

Tools>Internet Options>Content>Certificates>Trusted Root Certification Authorities>Import>Select Thawte Test Root.cer>Next, Next, Finish.

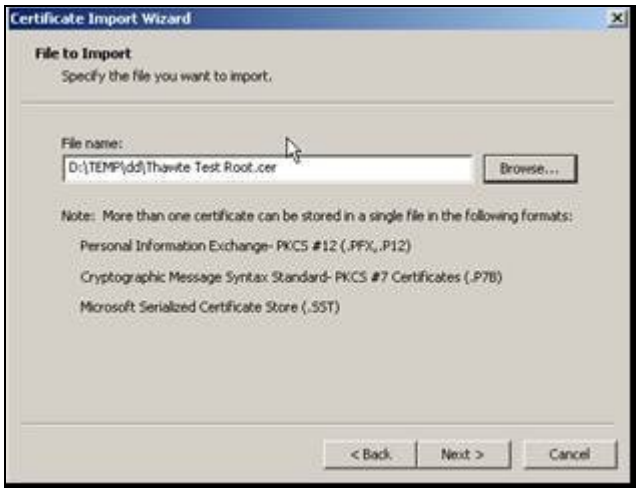


Figure 23: Importing a Thawte Certificate

5. Using the TFTP server, upload the **web_ssl.key and web_ssl.crt** files into the Midspan's secured Web server (refer to Section 3.3 or Section 4.4 for details).

6. Reopen your Web browser and browse to IP address (192.168.0.50), to one of the configuration Web pages (it is assumed that Midspan SSL option was already selected).

7. Click the ***lock*** icon to view certificate details and expiration date (21 days).

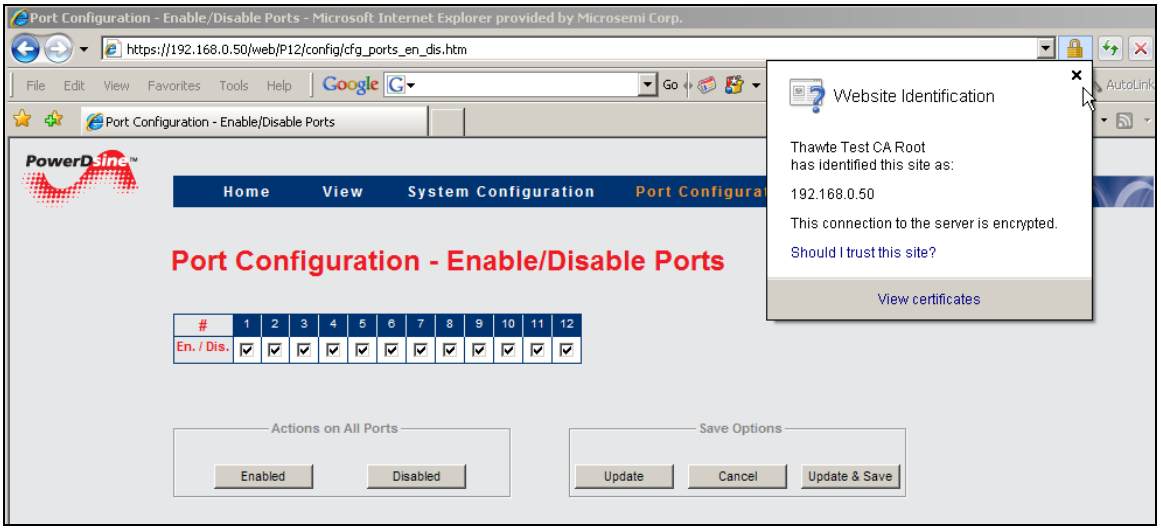


Figure 24: Viewing the Certificate

6. Appendix B: Evaluating a VeriSign Certificate

VeriSign offers an option to obtain a free SSL trial certificate which is good for 14 days. The following procedure describes how to download and install this certificate.

6.1. Creating the Certificate

1. Execute **01_generate_private_key.bat**.

   The **web_ssl.key** private key is created

2. Execute **02_create_certificate_request.bat**.

3. Enter the following information

Country Name (2 letter code) [AU] :	**US**
State or Province Name (full name) [Some-State] :	**MyState**
Locality Name (e.g., city) [] :	**MyCity**
Organization Name (for example company) [Internet Widgits Pty Ltd]:	**MyOrganization**
Organizational Unit Name (for example, section) []:	**MyUnit**
Common Name (for example **YOUR** name) []:	**192.168.0.50**
Email Address []:	
Enter the following 'extra' attributes to be sent with your certificate request	
A challenge password []:	
An optional company name []	

Must match Midspan IP Address

   The **web_ssl.csr** file is created.

4. Browse to *verisign - free ssl trial*.
5. Fill in the details and click **Continue**.
6. In the page that appears, click **continue**
7. Fill in the **Technical Contact** information and click **continue.**
8. From the **Server Platform** drop-down list, select the **Server not in list** option.
9. From the **What do you plan to use this SSL Certificate for? (optional)** drop-down list, select Other.
10. In Notebook, open and copy the **web_ssl.csr** file.
11. Paste the file into text box and click **Continue**.
12. Click **Continue**.
13. Fill in the **Challenge** phrase information and click **Continue**.
14. Click **Accept**.

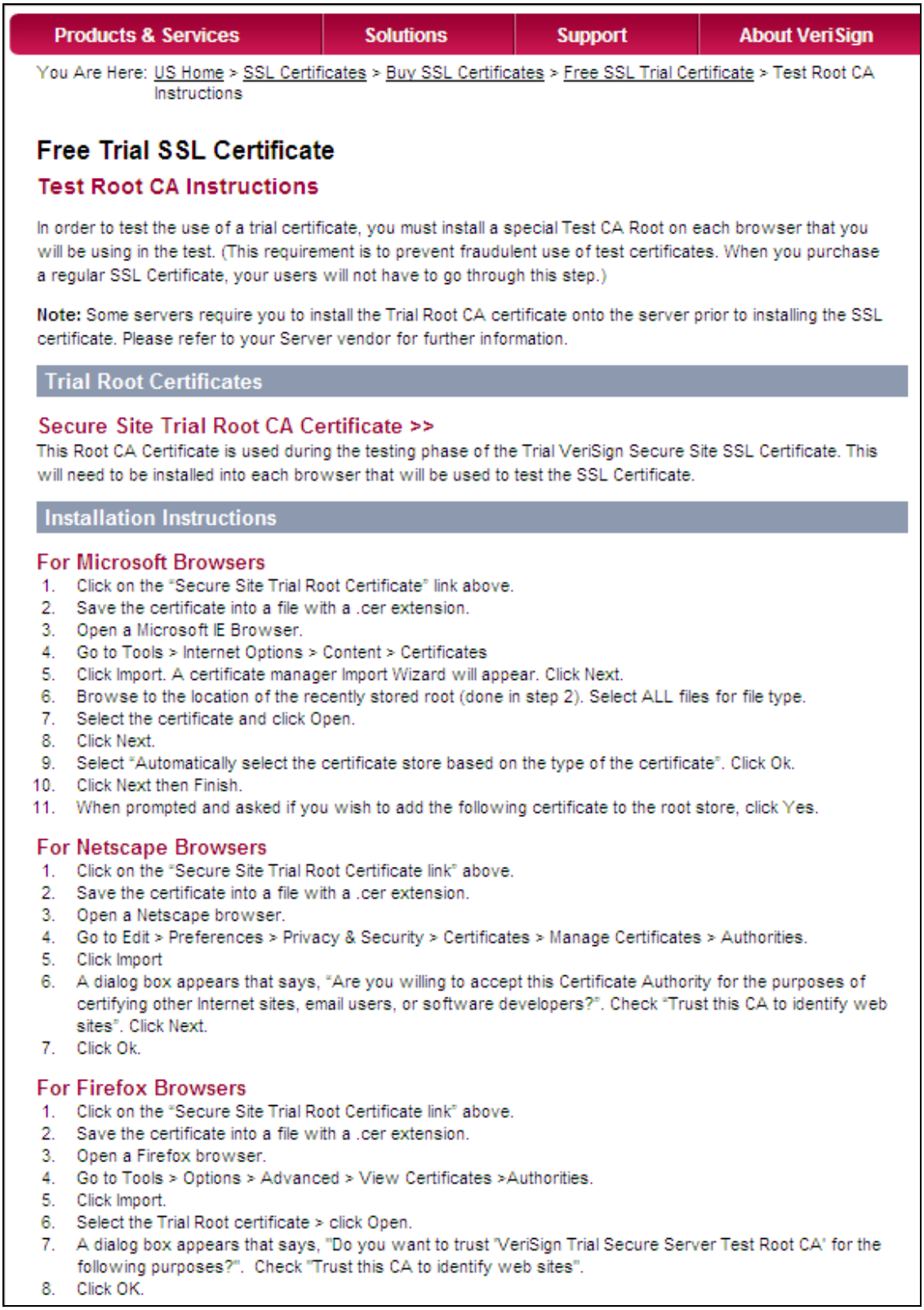
    Your Trial SSL Certificate and installation instructions will be sent to you via email.

Copy the created certificate text to file named ***web_ssl.crt***.

The certificate you had received is signed by VeriSign certificate authority. However the certificate still has to be installed on your Web browser (evaluation version).

6.2. Uploading the Certificate

Detailed instructions on how to upload the VeriSign certificate can be found at *verisign-test-root-ca* (Figure 25)
.



Products & Services | Solutions | Support | About VeriSign

You Are Here: US Home > SSL Certificates > Buy SSL Certificates > Free SSL Trial Certificate > Test Root CA Instructions

Free Trial SSL Certificate

Test Root CA Instructions

In order to test the use of a trial certificate, you must install a special Test CA Root on each browser that you will be using in the test. (This requirement is to prevent fraudulent use of test certificates. When you purchase a regular SSL Certificate, your users will not have to go through this step.)

Note: Some servers require you to install the Trial Root CA certificate onto the server prior to installing the SSL certificate. Please refer to your Server vendor for further information.

Trial Root Certificates

Secure Site Trial Root CA Certificate >>

This Root CA Certificate is used during the testing phase of the Trial VeriSign Secure Site SSL Certificate. This will need to be installed into each browser that will be used to test the SSL Certificate.

Installation Instructions

For Microsoft Browsers

1. Click on the "Secure Site Trial Root Certificate" link above.
2. Save the certificate into a file with a .cer extension.
3. Open a Microsoft IE Browser.
4. Go to Tools > Internet Options > Content > Certificates
5. Click Import. A certificate manager Import Wizard will appear. Click Next.
6. Browse to the location of the recently stored root (done in step 2). Select ALL files for file type.
7. Select the certificate and click Open.
8. Click Next.
9. Select "Automatically select the certificate store based on the type of the certificate". Click Ok.
10. Click Next then Finish.
11. When prompted and asked if you wish to add the following certificate to the root store, click Yes.

For Netscape Browsers

1. Click on the "Secure Site Trial Root Certificate link" above.
2. Save the certificate into a file with a .cer extension.
3. Open a Netscape browser.
4. Go to Edit > Preferences > Privacy & Security > Certificates > Manage Certificates > Authorities.
5. Click Import
6. A dialog box appears that says, "Are you willing to accept this Certificate Authority for the purposes of certifying other Internet sites, email users, or software developers?". Check "Trust this CA to identify web sites". Click Next.
7. Click Ok.

For Firefox Browsers

1. Click on the "Secure Site Trial Root Certificate link" above.
2. Save the certificate into a file with a .cer extension.
3. Open a Firefox browser.
4. Go to Tools > Options > Advanced > View Certificates >Authorities.
5. Click Import.
6. Select the Trial Root certificate > click Open.
7. A dialog box appears that says, "Do you want to trust 'VeriSign Trial Secure Server Test Root CA' for the following purposes?". Check "Trust this CA to identify web sites".
8. Click OK.

Figure 25: VeriSign Test CA Root Certificate

1. Using the TFTP, upload the **web_ssl.key** and **web_ssl.crt** files into the Midspan's secured Web server as detailed in Section 4.3.

2. Reopen your Web browser and browse to IP address 192.168.0.50, to one of the configuration Web pages (it is assumed that Midspan SSL option was already selected).

3. Click the **lock** icon to view certificate details and expiration date (14 days).

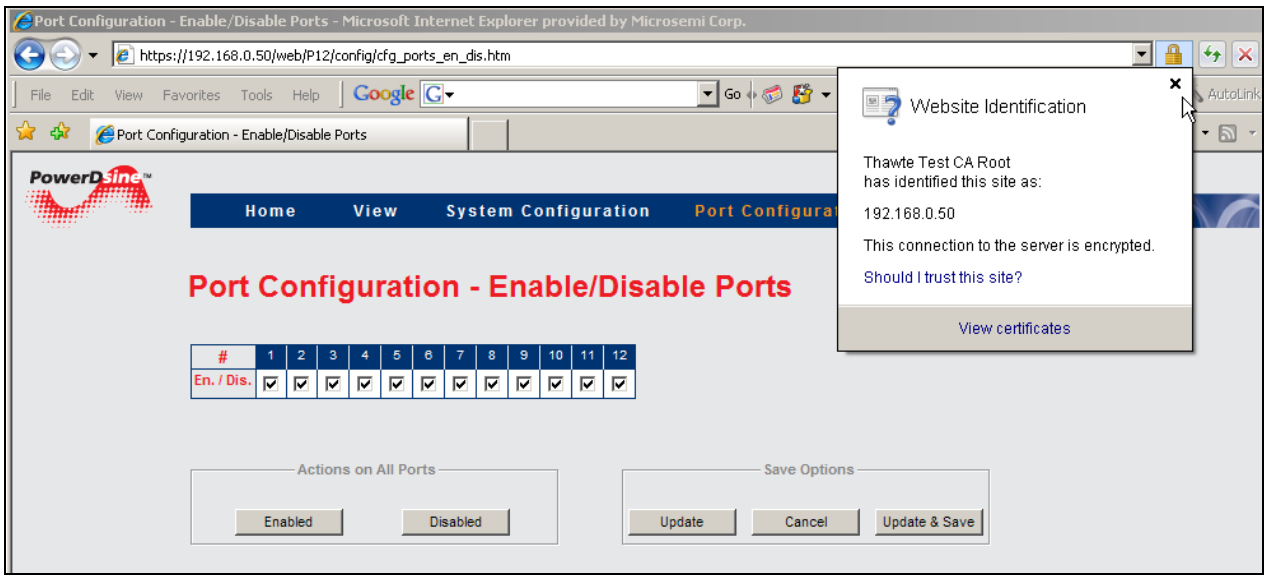


Figure 26: Viewing the Certificate

Revision History

Revision Level / Date	Para. Affected	Description
1.0 / 15-June-09	-	Initial Release
1.1 / 31 Aug 09		Logo, address
1.2 / 15-Sep-09		Formatting, English, restructured
1.3 / 14-Nov-11		Formatting, English, restructured

For support contact: customer.care_AMSG@microsemi.com

Visit our website at: www.microsemi.com/powerdsine **Catalog Number: 06-0059-056**