

PDS-104G - Secured web browsing certificate management

User Guide



TABLE OF CONTENTS

1	INTRODUCTION	2
1.1	GENERAL.....	2
1.2	ENFORCING SECURED WEB BROWSING.....	2
1.3	SECURED WEB BROWSING OPTIONS	2
1.3.1	<i>Browsing the unit over HTTPS using the unit's default self-signed certificate.....</i>	<i>2</i>
1.3.2	<i>Self-signed unit certificate</i>	<i>2</i>
1.3.3	<i>CA (Certificate Authority) signed certificate</i>	<i>3</i>
2	CERTIFICATE MANAGEMENT - PACKAGE TOOLS DESCRIPTION	3
2.1	PACKAGE CONTENT	3
2.1.1	<i>Self-Signed Certificate Authority.....</i>	<i>3</i>
2.1.2	<i>CA-Signed Certificate Authority</i>	<i>3</i>
3	EXAMPLE OF CREATING SELF-SIGNED CERTIFICATE	4
3.1	CREATING SELF-SIGNED CERTIFICATE AUTHORITY FILE.....	4
3.2	UPLOADING THE SELF-SIGNED TRUSTED ROOT CERTIFICATION AUTHORITY FILE TO THE WEB BROWSER	6
3.3	CREATING DEVICE-SPECIFIC CERTIFICATE	7
3.4	UPLOADING SELF-SIGNED CERTIFICATE TO THE UNIT	7
3.5	SELF-SIGNED CERTIFICATE VALIDATION.....	8
4	EXAMPLE OF CREATING CA-SIGNED CERTIFICATE.	9
4.1	GENERATING PRIVATE KEY.....	9
4.2	GENERATING CERTIFICATE REQUEST	10
4.3	SIGNING CERTIFICATE REQUEST	10
4.4	FINALIZING THE UNIT CERTIFICATE PROCESS	11
4.5	UPLOADING CA-SIGNED CERTIFICATE TO THE UNIT.....	11

1 INTRODUCTION

1.1 General

This document describes how to create, upload and manage self-signed/CA signed certificate for the PDS-104G unit. Both SSL and TLS security protocols are supported by the unit, although only TLSv1.1 and above is supported by recent web browsers.



NOTE:

Heartbleed security flow found in OpenSSL on 2014 was the drive behind abandoning SSLv3 by all web browsers, adopting TLSv1.1 or higher instead.

1.2 Enforcing secured web browsing

To enforce secure web browsing, enable **Web SSL Encryption** from within the configuration web page as in Figure 1.



The screenshot shows the Microsemi Configuration web interface. At the top, there are tabs for 'Main', 'Configuration', and 'Advanced'. The 'Configuration' tab is selected. Below the tabs, the title 'Security Configuration' is displayed. Under this title, there is a section titled 'Username and Password' with fields for 'User Name' (containing 'admin'), 'Password' (masked with dots), and 'Confirm Password' (masked with dots). Below these fields, there is a dropdown menu for 'Telnet / SSH' set to 'Telnet'. At the bottom of this section, there is a checkbox for 'Web SSL Encryption' which is checked. A red arrow points to this checkbox.

Figure 1

1.3 Secured Web Browsing options

There are several methods to secure web browsing, of which CA signed certificates is the most secured.

1.3.1 Browsing the unit over HTTPS using the unit's default self-signed certificate

Advantage – The simplest method, requiring no extra preparations by the IT manager.

Disadvantage – A warning message displayed by the browser, encouraging the user to exit the website unless he is absolutely sure that this is a trusted website. This method is not recommended although it works well for closed networks and devices using absolute IP address.

1.3.2 Self-signed unit certificate

Advantage – No need to pay for every device certificate, and having full control over the certificate's creation and expiration date.

Disadvantage – A self-generated trusted root authority certificate has to be uploaded to every PC/Laptop to be used for browsing the unit over SSL/TLS. Failing to do so will cause the web browser to issue the same warning, advising the user to leave the website since it is not secured.

1.3.3 CA (Certificate Authority) signed certificate

Advantage – The recommended method used by many websites such as Amazon, eBay, etc.

Disadvantage – An annual fee for every certificate signed by the CA. Examples of trusted CA are VeriSign, Symantec, Thawte, etc.

2 CERTIFICATE MANAGEMENT - PACKAGE TOOLS DESCRIPTION

2.1 Package content

The certificate management package is based on an open-source OpenSSL tool, and readymade batch files to ease user interaction with the Open SSL tool. For ease of use, two separate sub folders are available.

2.1.1 Self-Signed Certificate Authority

This folder contains the OpenSSL tool plus two batch files.

1. The first batch file is named **01_Create Trusted Root Certification Authority (done once).bat**. It is used to create Trusted Root Certification Authority which is usually done only once, and has to be uploaded to every web browser used for browsing the PDS-104G unit over HTTPS
2. The 2nd batch file is named **02_Create Certificate for each Device.bat**. It is used to generate a certificate for every PDS-104G unit in use (the certificate is IP dependent, and since every device has its own IP, a unique certificate has to be created for every device).

2.1.2 CA-Signed Certificate Authority

This folder contains the OpenSSL tool plus three batch files.

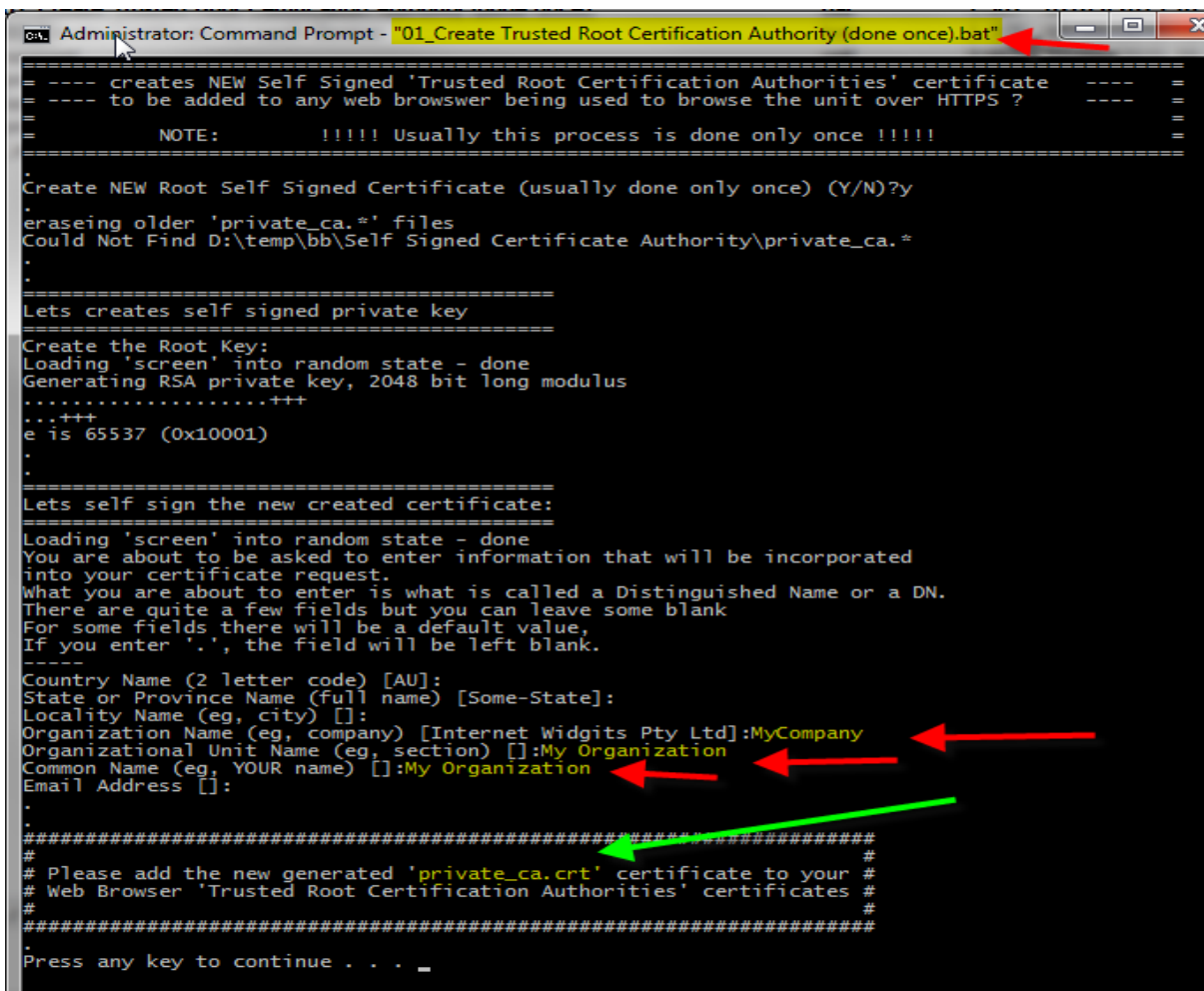
1. The 1st batch file named **01_generate_private_key.bat** is used to create a 2048-bit long private key. Typically, private key generation is done only once.
2. The 2nd batch file named **02_create_certificate_request.bat** is used to create a certificate request to be uploaded to trusted root certificate authorities such as VeriSign, etc. The 2nd batch file has to be executed for every network device to be managed over HTTPS.
3. The 3rd batch file named **03_create_certificate.bat** is used to combine the certificate received back from the certificate authority site such as VeriSign (with a .crt extension) together with the private key file (key extension) we generated using the first batch file, into a single file with a .pem extension, to be uploaded back to the PDS-104G unit.

3 EXAMPLE OF CREATING SELF-SIGNED CERTIFICATE

This example assumes the unit IP is 192.168.0.50.

3.1 Creating self-signed Certificate Authority file

Run batch file **01_Create Trusted Root Certification Authority (done once).bat**. The batch file will create a 2048-bit private key file named **private_ca.key** with expiration date of 10 years (3650 days), which can be easily changed by modifying the batch file. Next, the user will be requested to fill in various fields as in Figure 2, after which it will generate file named **private_ca.crt**, which is the self-signed trusted authority certificate file required to be uploaded to every web browser being used to browse the unit over the Network using HTTPS secured protocol.



```

Administrator: Command Prompt - "01_Create Trusted Root Certification Authority (done once).bat"
=====
---- creates NEW Self Signed 'Trusted Root Certification Authorities' certificate ----
---- to be added to any web browser being used to browse the unit over HTTPS ? ----
=====
NOTE:      !!!!! Usually this process is done only once !!!!!
=====
Create NEW Root Self Signed Certificate (usually done only once) (Y/N)?y
erasing older 'private_ca.*' files
Could Not Find D:\temp\bb\Self Signed Certificate Authority\private_ca.*
.
.
=====
Lets creates self signed private key
=====
Create the Root Key:
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
.....+++
...+++
e is 65537 (0x10001)
.
.
=====
Lets self sign the new created certificate:
=====
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:MyCompany
Organizational Unit Name (eg, section) []:My Organization
Common Name (eg, YOUR name) []:My Organization
Email Address []:
.
.
#####
# Please add the new generated 'private_ca.crt' certificate to your #
# Web Browser 'Trusted Root Certification Authorities' certificates #
#####
Press any key to continue . . . _

```

Figure 2



NOTE:

The batch file **01_Create Trusted Root Certification Authority (done once).bat** should be typically executed only once. Running it again will erase and replace the already created **private_ca.crt** file



3.2 Uploading the self-signed trusted root certification authority file to the web browser

Upload the *private_ca.crt* file to web browser **Trusted Root Certification Authorities** list. This procedure has to be repeated for every web browser used to browse the unit over HTTPS.

The example in figures 3, 4, 5 refers to *the Chrome* web browser. Each web browser has its own instructions on how to perform the same actions.

1. In Chrome, select **Settings**.
2. Scroll down and press on **Show Advanced Settings**.
3. Scroll down to HTTPS/SSL and select **Manage Certificates**.
4. Select the **Trusted Root Certification Authorities** tab.
5. Select **Import**, and select the *private_ca.crt* file.

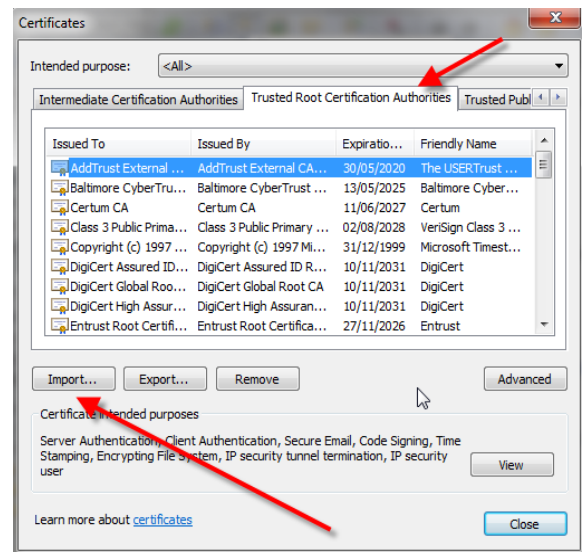


Figure 3

6. In the warning message that appears. Select **Yes**.
7. An **Import was Successful** message should appear.

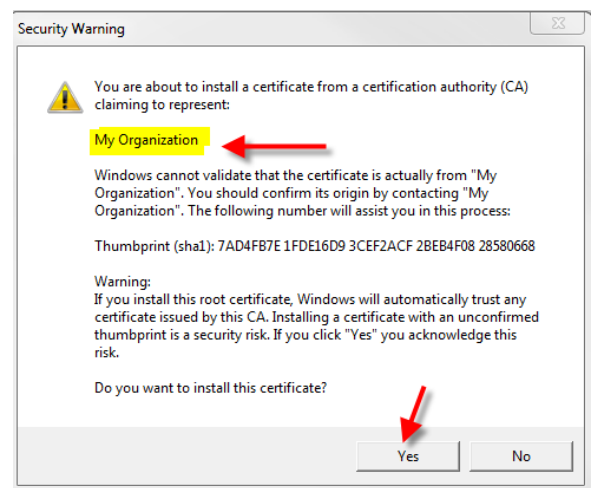


Figure 4

8. Browse again as in Figure 4 to **Trusted Root Certification Authority** list and verify that *My Organization* now appears on the list.

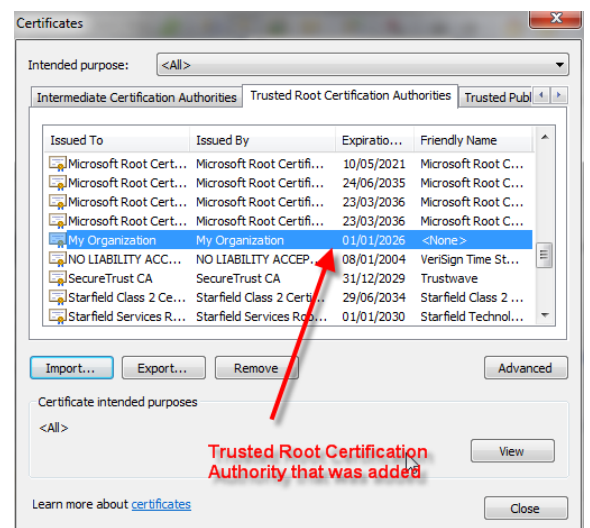


Figure 5

3.3 Creating device-specific certificate

1. Make sure the files **private_ca.key** and **private_ca.crt** which were created in the previous stage are in the same folder where the 2nd batch file is going to be executed.
2. Run **02_Create Certificate for each Device.bat** and fill in the various fields as in Figure 6.
Please note that the Common Name field must match the unit IP address.
3. Now upload the newly created **web_ssl.pem** certificate to the PDS-104G unit over TFTP as described in the next paragraph.

3.4 Uploading self-signed certificate to the unit

1. Run TFTP Server on one of the computers which are accessible by the PDS-104G unit on the network.
2. Place the file **web_ssl.pem** on the TFTP Server root folder.
3. Browse to the unit over Telnet/SSH (as was configured over the Web).
4. From the main menu, select the **Configuration and maintenance** menu.
5. Within the configuration menu select **Download WEB SSL Certificate from TFTP Server**.
6. From within the **Certificate Download** menu select **Download self-signed certificate**.
7. Now enter the TFTP Server IP address and certificate filename - **web_ssl.pem**.

```

erasing older 'web_ssl.*' files
Could Not Find D:\temp\bb\Self Signed Certificate Authority\web_ssl.*

=====
Lets create unique certificate per each Network Device
=====

Create private Key:
Loading 'screen' into random state - done
Generating RSA private key, 2048 bit long modulus
.....+++++
e is 65537 (0x10001)

=====
Lets generate certificate sign request:
NOTE - For 'Common Name' field please use device DNS name or IP address
=====

Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:My Company
Organizational Unit Name (eg, section) []:My Unit
Common Name (eg, YOUR name) []:192.168.0.50
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

=====
Lets sign the CSR. Please note that files 'private_ca.crt' and
'private_ca.key' must be present
=====
Loading 'screen' into random state - done
Signature ok
subject=/C=AU/ST=Some-State/O=My Company/OU=My Unit/CN=192.168.0.50
Getting CA Private Key

=====
Lets convert key and crt to pem format
=====
Loading 'screen' into random state - done
MAC verified OK

=====
Place file named 'web_ssl.pem' on TFTP Server root folder. Next connect to
your device using Telnet/SSH. From within configuration menu select the
option to upload self signed certificate into the device.
=====
Press any key to continue . . .

```

Figure 6

3.5 Self-Signed Certificate validation.

- Open Chrome web browser and browse to IP 192.168.0.50. The web browser will be redirected to <https://192.168.0.50>. No warning messages should appear in the web browser; only username and password request should appear.
- Green lock as in Figure 7 on the left side of the URL should indicate that the browsing to the unit is done over secured HTTPS protocol.

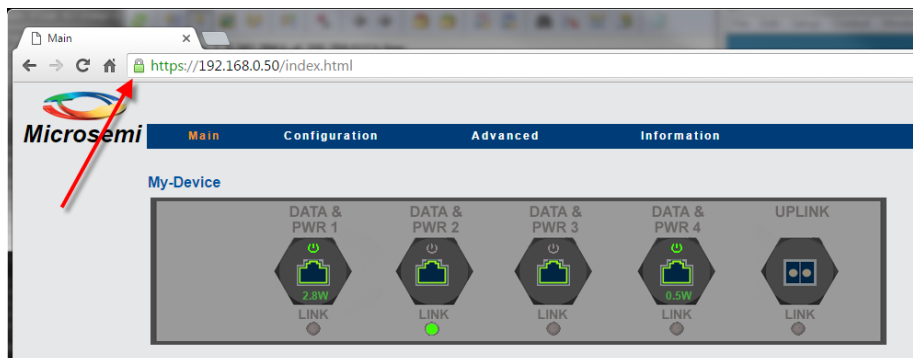


Figure 7

4 EXAMPLE OF CREATING CA-SIGNED CERTIFICATE.

A CA-signed certificate will be typically used whenever the unit is connected to the global public Internet. It has its own domain name as `www.my-unit.com`, and secure web browsing over the internet from any web browser is required without any extra steps from the remote end-user.

Only trusted root certificate authorities which are installed together with the web browser installation can be used to sign the certificate request which will be generated. The user has to pay yearly fee to the certificate authority organization in order to get a signed certificate, which will be typically limited to one or two years before it has to be updated. Examples of such companies are VeriSign, Symantec, Thawte, etc. See Figure 8 for additional examples.

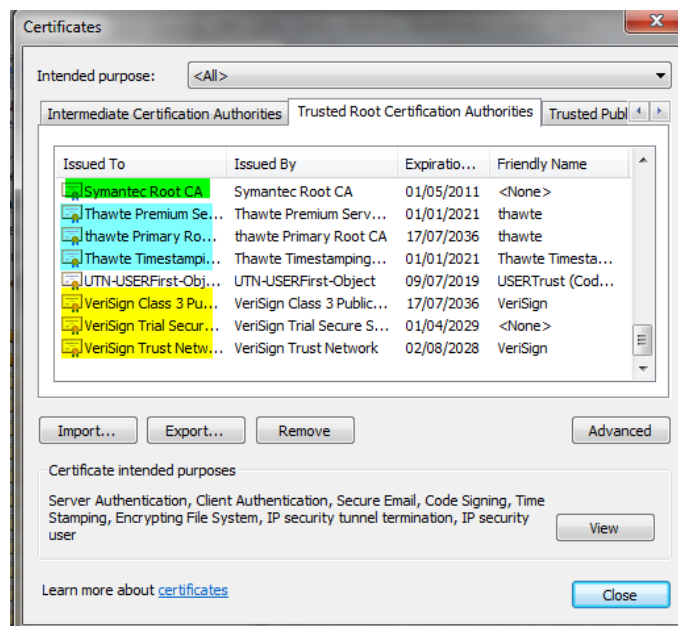


Figure 8

4.1 Generating private key

Run batch file **`01_generate_private_key.bat`**. The batch file will create 2048-bit private key named **`web_ssl.key`**.



NOTE:

The batch file **`01_generate_private_key.bat`** should be typically executed only once. Running it again will erase and replace the already created **`web_ssl.key`** file



4.2 Generating certificate request

Run batch file **02_create_certificate_request.bat**. After filling-in all the parameters as in Figure 9, a certificate-request file named **web_ssl.csr** will be created. Please note that under **Common Name** you must fill in the unit's domain name e.g., **www.my-unit.com** (there is no support for absolute IP address).

```

CA> Administrator: Command Prompt

=====
Lets creates certificate request (web_ssl.csr)
=====

Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:my-state
Locality Name (eg, city) []:my-city
Organization Name (eg, company) [Internet Widgits Pty Ltd]:My-Organization
Organizational Unit Name (eg, section) []:My-Unit
Common Name (eg, YOUR name) []:www.my-dns-name.com
Email Address []:my-email@my-email.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Press any key to continue...
D:\temp\bb\CA Signed Certificate Authority>

```

Figure 9

4.3 Signing certificate request

Upload **web_ssl.csr** certificate request to your favorite certificate authority organization. After paying the appropriate fees and filling-in all the required information you will be issued a certificate, similar to the one in Figure 10.

[illegible]

Figure 10

Copy the certificate provided by the CA to the file named **web_ssl.crt**, and place under the same folder where the 2nd batch file was executed.

4.4 Finalizing the unit certificate process

Run the 3rd batch file named **03_create_certificate.bat**, which will combine the **web_ssl.crt** and **web_ssl.key** files into a single file named **web_ssl.pem**.

4.5 Uploading CA-signed certificate to the unit

1. Run TFTP Server on one of the computers accessible to the PDS-104G unit over the Network.
2. Place the files **web_ssl.crt** and **web_ssl.pem** in the TFTP Server root folder.
3. Browse to the unit over Telnet/SSH (as was configured over the web).
4. From the main menu, select the **Configuration and maintenance** menu.
5. Within the configuration menu, select **Download WEB SSL Certificate from TFTP**.
6. From within the **Certificate Download** menu, select **Download CA issued certificate**.
7. Now enter the TFTP Server IP address, CA-signature file name (web_ssl.crt), and the device certificate file name (web_ssl.pem).
8. The unit will download both files and verify validity of both files against the unit internal web server. After successful validation, a success message as in Figure 11 should appear

```

Certificate Download Menu
-----
1. Download self-signed certificate
2. Download CA issued certificate
3. Restore to factory default certificate
ESC. Return to configuration menu

Download CA issued certificate - are you sure( Y/N, ESC ) ?
Enter TFTP server IP address or domain name: 192.168.0.40
Enter CA signature filename (as web_ssl.crt): web_ssl.crt
Enter Device certificate filename (as web_ssl.pem): web_ssl.pem
web_ssl.crt          100% |*****| 1468 0:00:00 ETA
web_ssl.pem          100% |*****| 3219 0:00:00 ETA
Download finished, loading Web Server with new configuration...
Success!

```

Figure 11



NOTE:

1. A success message doesn't necessary mean that the entire process was done correctly. It only indicates that the two uploaded files' content and format comply with the unit Web Server files format
2. In case any of the two uploaded files doesn't comply with the unit Web Server files format, the web server will discard the new uploaded certificate files and will continue to use the already existing certificate files



Microsemi

The information contained in the document (unless it is publicly available on the Web without access restrictions) is PROPRIETARY AND CONFIDENTIAL information of Microsemi and cannot be copied, published, uploaded, posted, transmitted, distributed or disclosed or used without the express duly signed written consent of Microsemi. If the recipient of this document has entered into a disclosure agreement with Microsemi, then the terms of such Agreement will also apply. This document and the information contained herein may not be modified, by any person other than authorized personnel of Microsemi. No license under any patent, copyright, trade secret or other intellectual property right is granted to or conferred upon you by disclosure or delivery of the information, either expressly, by implication, inducement, estoppels or otherwise. Any license under such intellectual property rights must be approved by Microsemi in writing signed by an officer of Microsemi.

Microsemi reserves the right to change the configuration, functionality and performance of its products at anytime without any notice. This product has been subject to limited testing and should not be used in conjunction with life-support or other mission-critical equipment or applications. Microsemi assumes no liability whatsoever, and Microsemi disclaims any express or implied warranty, relating to sale and/or use of Microsemi products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Any performance specifications believed to be reliable but are not verified and customer or user must conduct and complete all performance and other testing of this product as well as any user or customer final application. User or customer shall not rely on any data and performance specifications or parameters provided by Microsemi. It is the customer's and user's responsibility to independently determine suitability of any Microsemi product and to test and verify the same. The information contained herein is provided "AS IS, WHERE IS" and with all faults, and the entire risk associated with such information is entirely with the User. Microsemi specifically disclaims any liability of any kind including for consequential, incidental and punitive damages as well as lost profit. The product is subject to other terms and conditions which can be located on the web at <http://www.microsemi.com/company/terms-and-conditions>.

Revision History

Revision Level / Date	Para. Affected	Description
1.0		Initial release

© 2016 Microsemi Corp.

All rights reserved.

For support contact: PoEsupport@microsemi.com

Visit our web site at: <http://www.microsemi.com/products/poe-systems/poe-systems>

Document Catalog Number: PDS-104G - SECURED WEB BROWSING CERTIFICATE MANAGEMENT