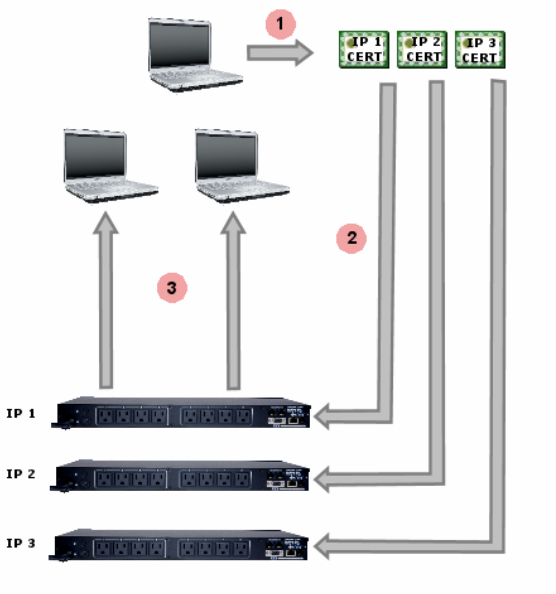
iBootBar
Certificate Utility

Overview

The Certificate Utility (CUU.exe) is designed to create and distribute Secure Socket Layer (SSL) certificates to iBootBars and the PCs that communicate them. Although the iBootBar comes from the factory with a certificate installed, this certificate common name is Dataprobe iBB, and will generate a warning message when connecting to the iBootBar when using SSL. For most customers, this error message can be easily ignored and secure connection to the iBootBar continues. For customers with special circumstances, the CU was designed to facilitate creation and distribution of SSL Certificates tailored to a specific iBootBar, eliminating the error message entirely. There are two methods that can be used to create and distribute the certificates

1. **Self Signed Certificates.** A Self-signed certificate is the most common approach. In this approach, the CU generates multiple certificates, each unique and based on the IP address, or DNS name of each iBootBar. The CU also provides the means to install the certificate on the iBootBar, making it easy to generate and distribute. Upon initial connection to the iBootBar, the user will be offered an opportunity to install the certificate from the iBootBar. This is done once for each browser on the PC and each iBootBar.



Self Sign Method

Step 1: Using the CU, create one unique Certificate based on the IP Address of each iBootBar.

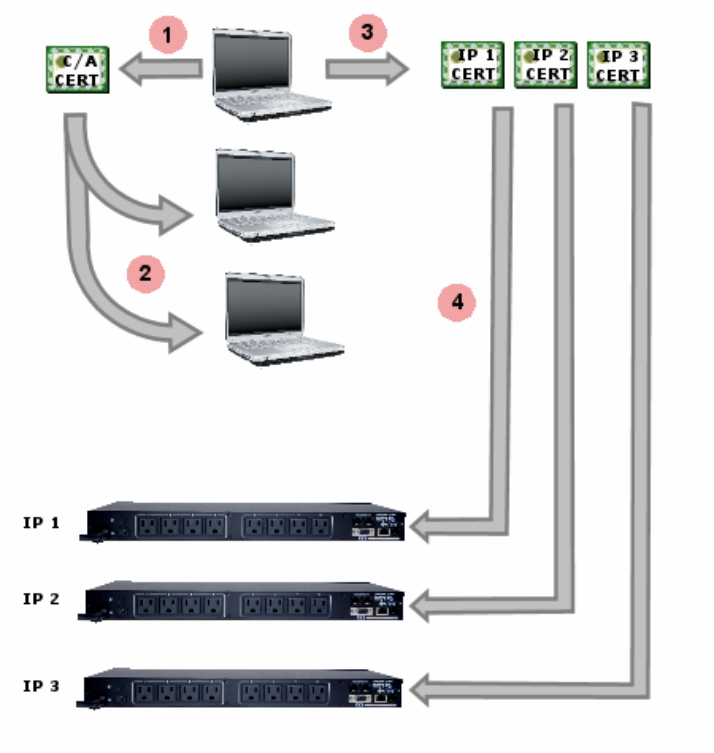
Step 2: Use the CU to upload the Certificates to each iBoot Bar

Step 3: Upon connecting to the iBootBar, each PC accepts the certificate installed in the iBootBar.

REF: iBootBar_CertUtil_v080320e

Technical Support: 201-934-5111 tech@dataprobe.com
Main: 201-934-9944 Website: dataprobe.com

2. **Root Certificate Authority.** The Root Certificate Authority method pre installs the certificates required in both the PC and the iBootBar. This eliminates the need for accepting the certificate from each iBootBar on each PC. The Root Certificate is generated and installed in each PC prior to communication with the iBootBar. The Root Certificate also is used, along with the IP address or domain of the iBootBar, to generate the certificates that are installed in the iBootBar.



Root Certificate Authority Method

Step 1: Create A Root Certificate Authority (CA) using the Certificate Upload Utility (CU).

Step 2: Install the CA into any PCs that need to communicate with the iBootBars.

Step 3: Create certificates for each iBootBar using the CU. Each certificate is unique and based on the C/A and the iBootBars IP Address or domain name.

Step 4: Install the certificate into the iBootBar(s) using the CU.

Method 1. Self Signed Certificates

Step 1. Create a Self Signed Certificate

a. Open the CU

b. Click on Create a Self Signed Certificate

c. Click Next

d. Enter the Required Information about the Self Signed Certificate in the fields as shown.

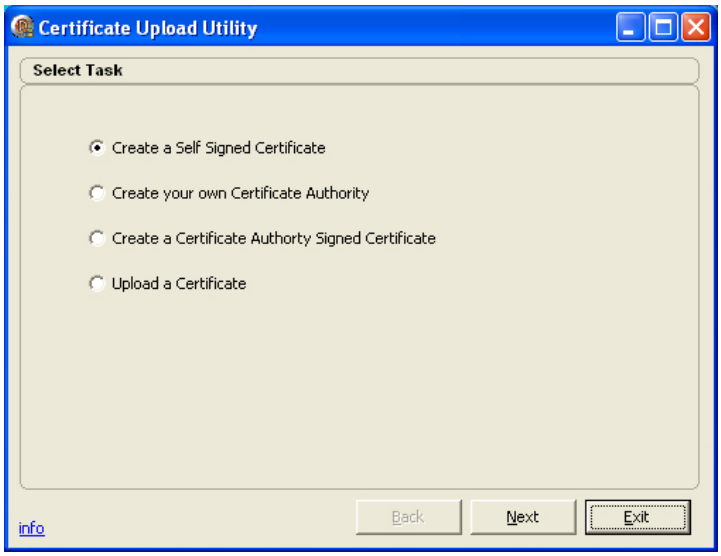
Certificate Name: This is the filename for the certificate.
Common Name: Usually the IP address of the iBootBar that that will use the certificate

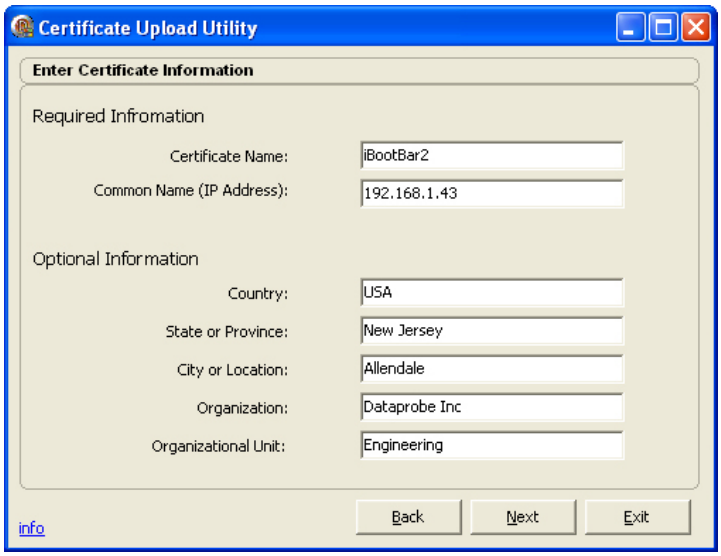
e. Enter the Optional Information if desired

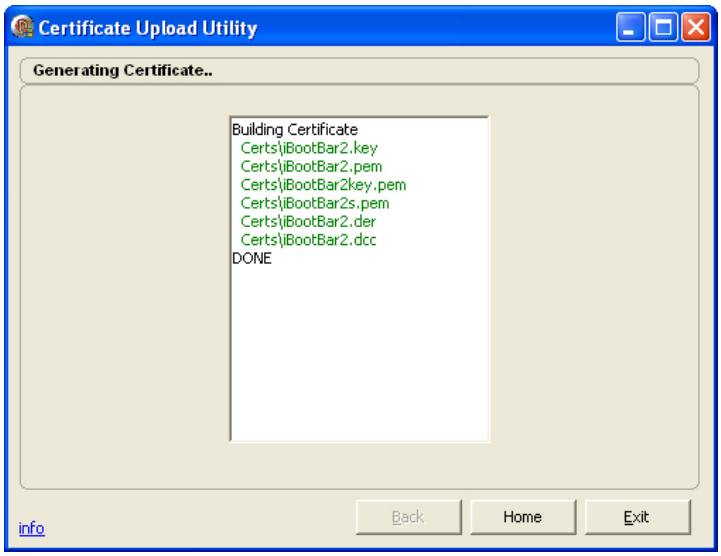
f. Click Next when done

g. The CU will generate the required files and store them in the <install_directory/Certs> subdirectory.*

h. Click Home when Done.







* Vista Users: See Appendix A for file location information

Step 2. Upload the Certificate to the iBootBar

a. Open the CU (in necessary)

b. Click on Upload a Certificate

c. Click Next

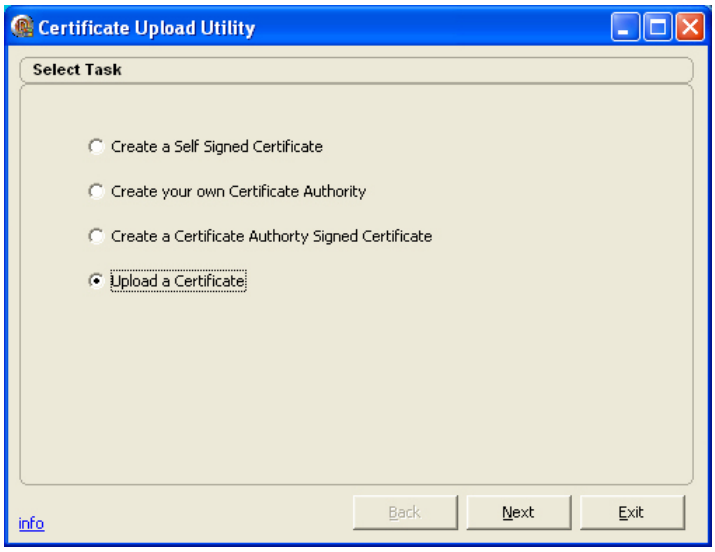
d. Enter or Browse to the location of the certificate files. The default location is <install_directory\Certs\>

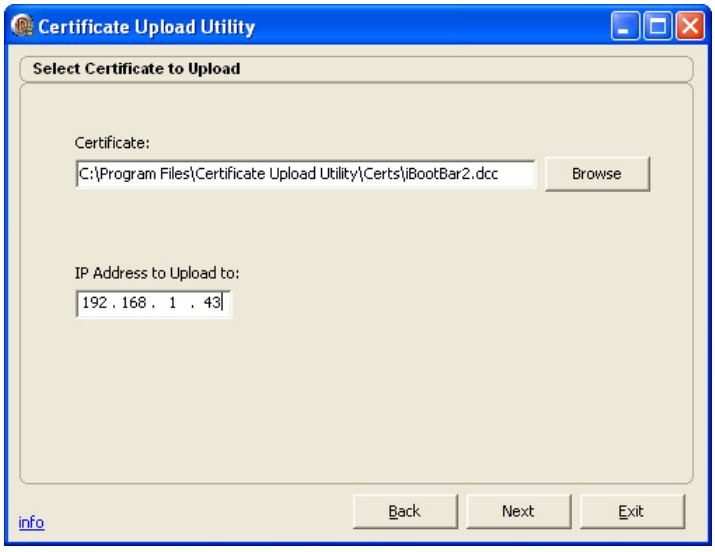
e. Enter the IP address of the iBootBar to upload the certificate to.

f. Click on Next

g. The certificate upload progress is displayed. When complete, Click Home

h. After receiving the certificate, the iBootBar needs to be rebooted, via the CLI (Telnet, Serial) or the front panel switch. This will not affect the status of the outlets.





Step 3. Use the Certificate in a Browser.

Internet Explorer

Upon connection to the iBootBar with the new certificate, the following warning will be displayed.

<u>If you click on Yes:</u> The certificate will be installed for this session only. Each time you access this iBootBar, the same warning will be displayed.

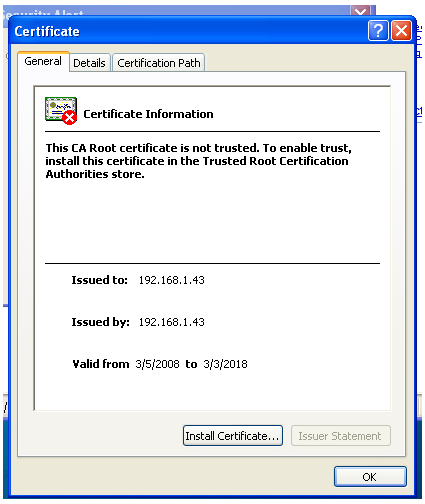
<u>To permanently install this certificate:</u>

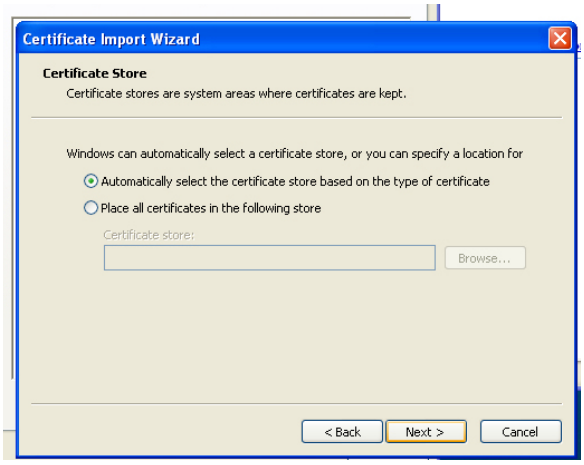
a. Click on View Certificate

b. Click on Install Certificate. The import wizard will begin. Click on Next

c. Select Certificate Store location. Automatic is preferred.

d. Review and accept the Security Warning. Click Yes to install the certificate permanently





Firefox

a. Upon connection, select either

Accept this certificate permanently or
Accept this certificate temporarily for this session.

b. Click OK

Method 2. Root Certificate Authority

Step 1. Create a Root Certificate Authority

a. Open the CU

b. Click on Create your own Certificate Authority

c. Click Next

d. Enter the Required Information about the Self Signed Certificate in the fields as shown.

Certificate Name: This is the filename for the certificate.
Common Name: This name identifies the Certificate to the web browser. Choose a name that will identify its source.

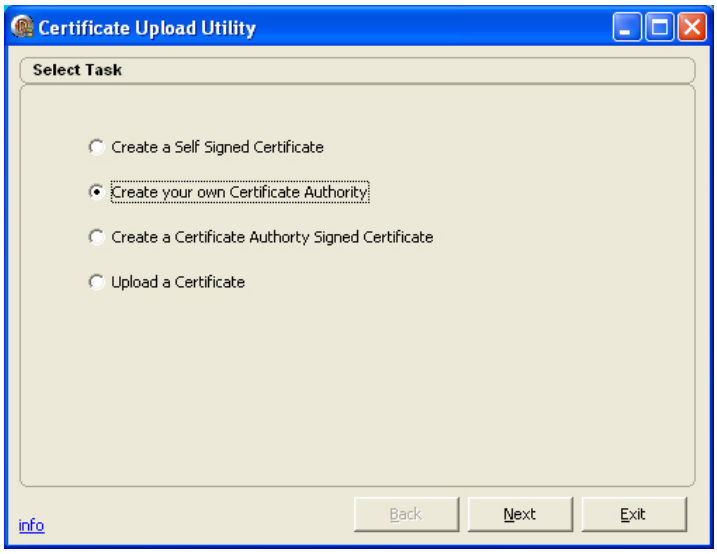
e. Enter the Optional Information if desired

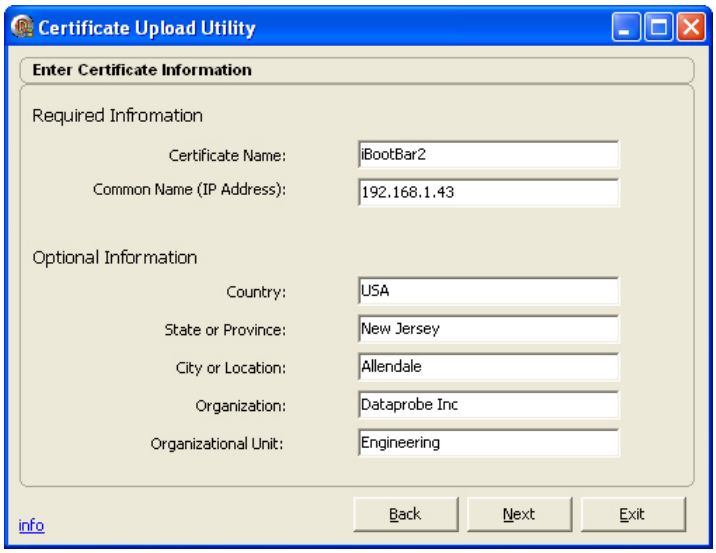
f. Click Next when done

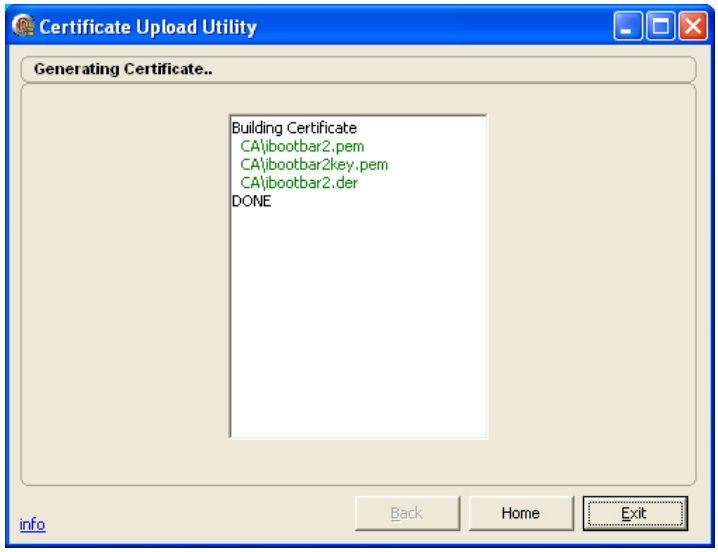
g. The CU will generate the required files and store them in the <install_directory/CA> subdirectory.*

h. Click Home when Done.

i. Install the Root Certificate into you Browser







Step 2. Install the Root Authority Certificate into one or more PCs Using Internet Explorer

a. Navigate to the location of the Root Certificate

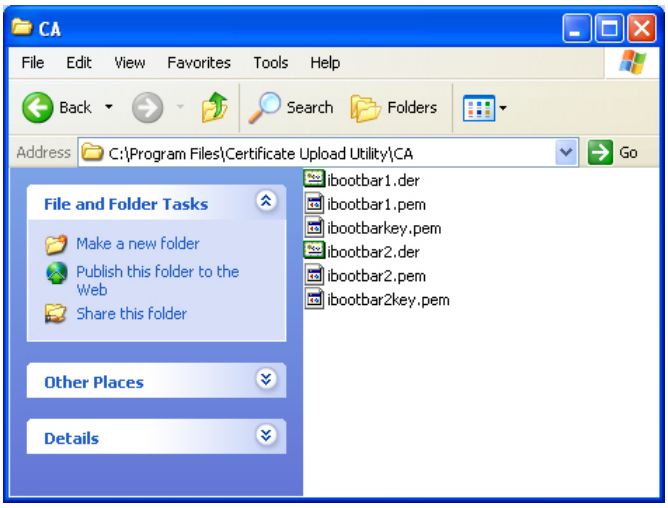
b. Double click on the .der file matching the filename of the certificate.

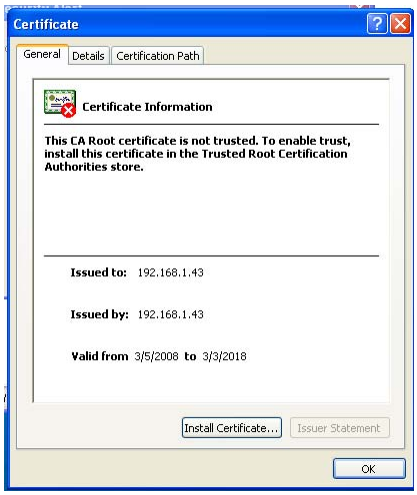
c. Click on Install Certificate. The import wizard will begin. Click on Next

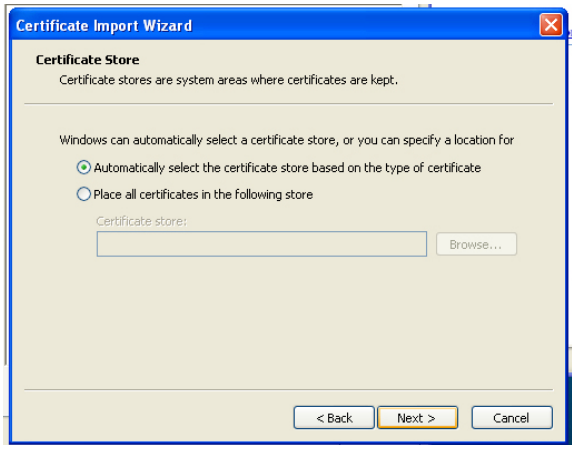
d. Select Certificate Store location. Automatic is preferred.

e. Review and accept the Security Warning. Click Yes to install the certificate permanently.

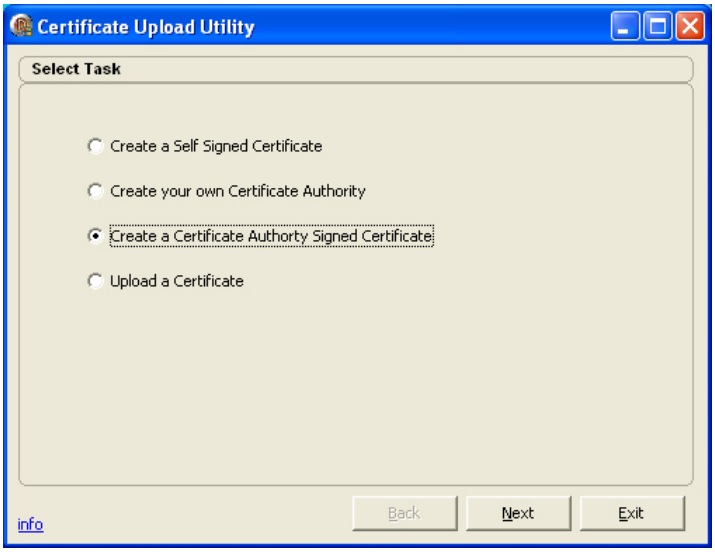
Repeat step two for all PCs that need to communicate securely with the iBootBars. Copy the three files created in this step to each of the PCs and install the Root Authority Certificate in each.







Step 3. Create Certificates for each iBootBar using the Root Authority Certificate.

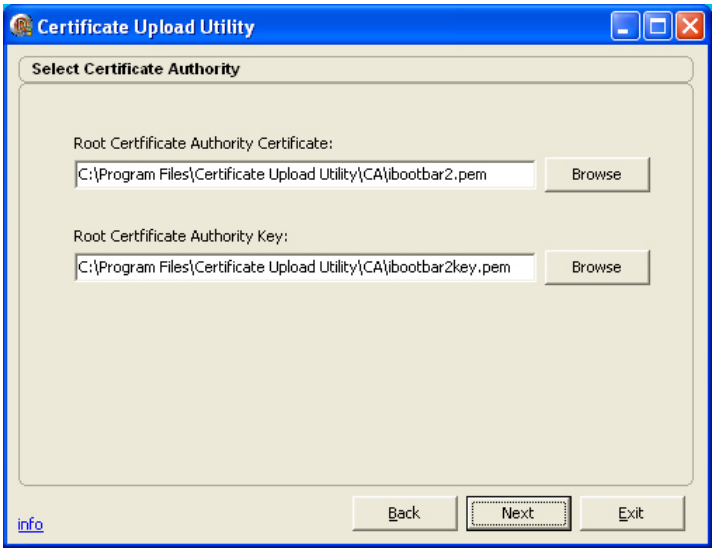


a. Open the CU

b. Click on Create a Certificate Authority Signed Certificate

c. Click Next

d. Enter or Browse to the Root Certificate Authority file location (default is <install_directory/CA>* and select the .pem file matching the name of the Certificate Authority created above.



e. Enter or Browse to the key file (*key.pem) matching the name of the Certificate Authority created above.

f. Click Next

g. Enter the Required Information about the Certificate in the fields as shown.

Certificate Name: This is the filename for the certificate.
Common Name: Usually the IP address of the iBootBar that that will use the certificate.

h. Enter the Optional Information if desired

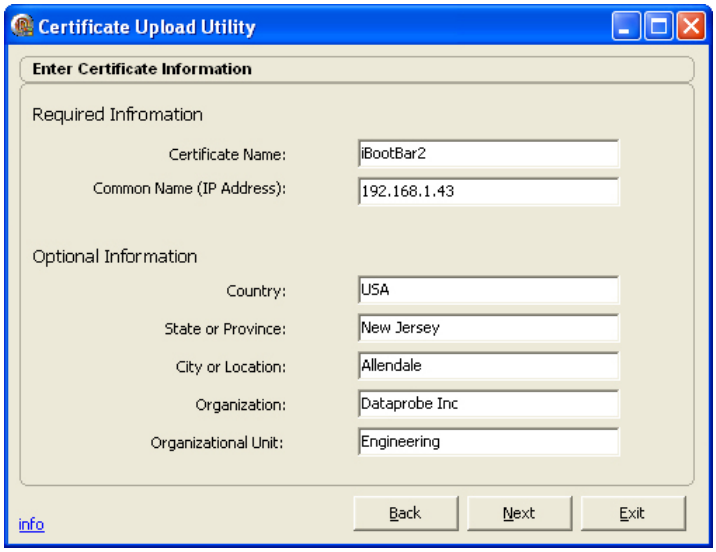
i. Click Next when done

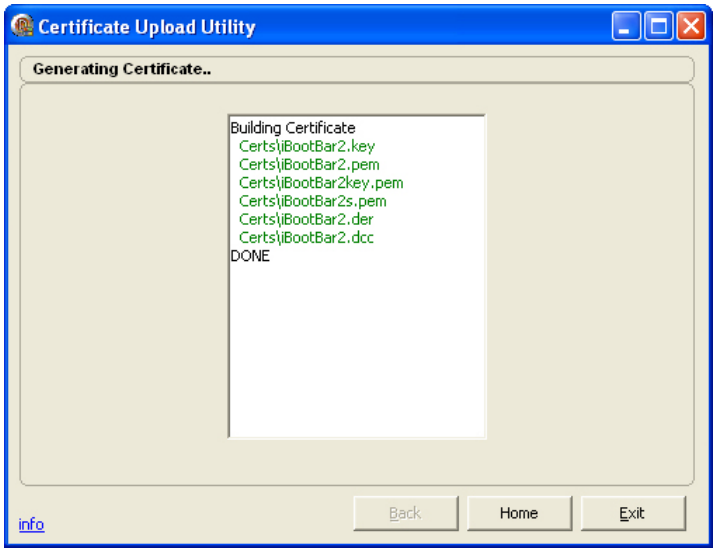
j. The CU will generate the required files and store them in the <install_directory/Certs> subdirectory.*

k. Click Home when Done.

Repeat Step 3 for each iBootBar.

* Vista Users: See Appendix A for file location information





Step 4. Upload the Certificate into the iBootBar

a. Open the CU (in necessary)

b. Click on Upload a Certificate

c. Click Next

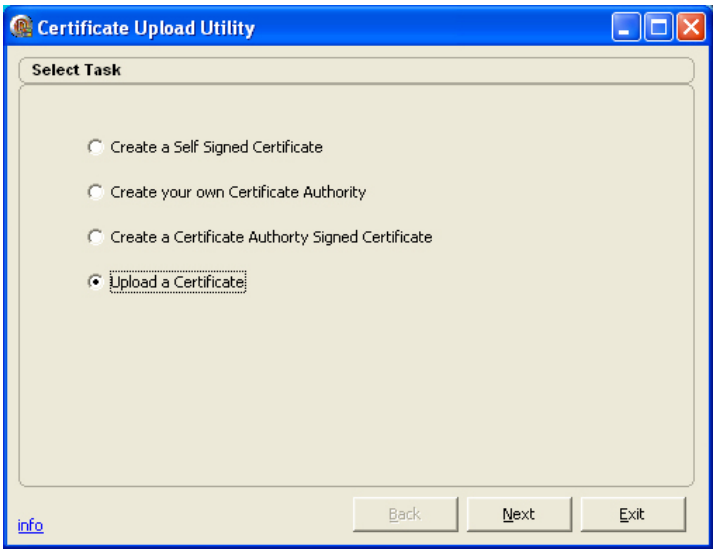
d. Enter or Browse to the location of the certificate files.

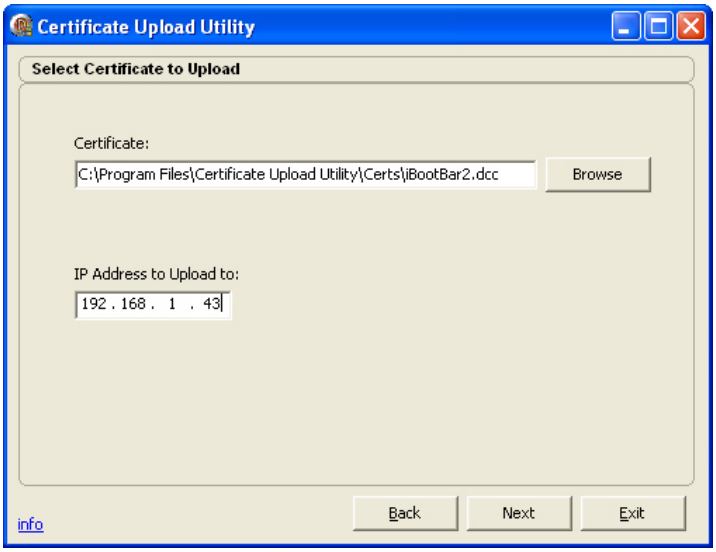
e. Enter the IP address of the iBootBar to upload the certificate to.

f. Click on Next

g. The certificate upload progress is displayed. When complete, Click Home

h. After receiving the certificate, the iBootBar needs to be rebooted, via Telnet or the front panel switch. This will not affect the status of the outlets.





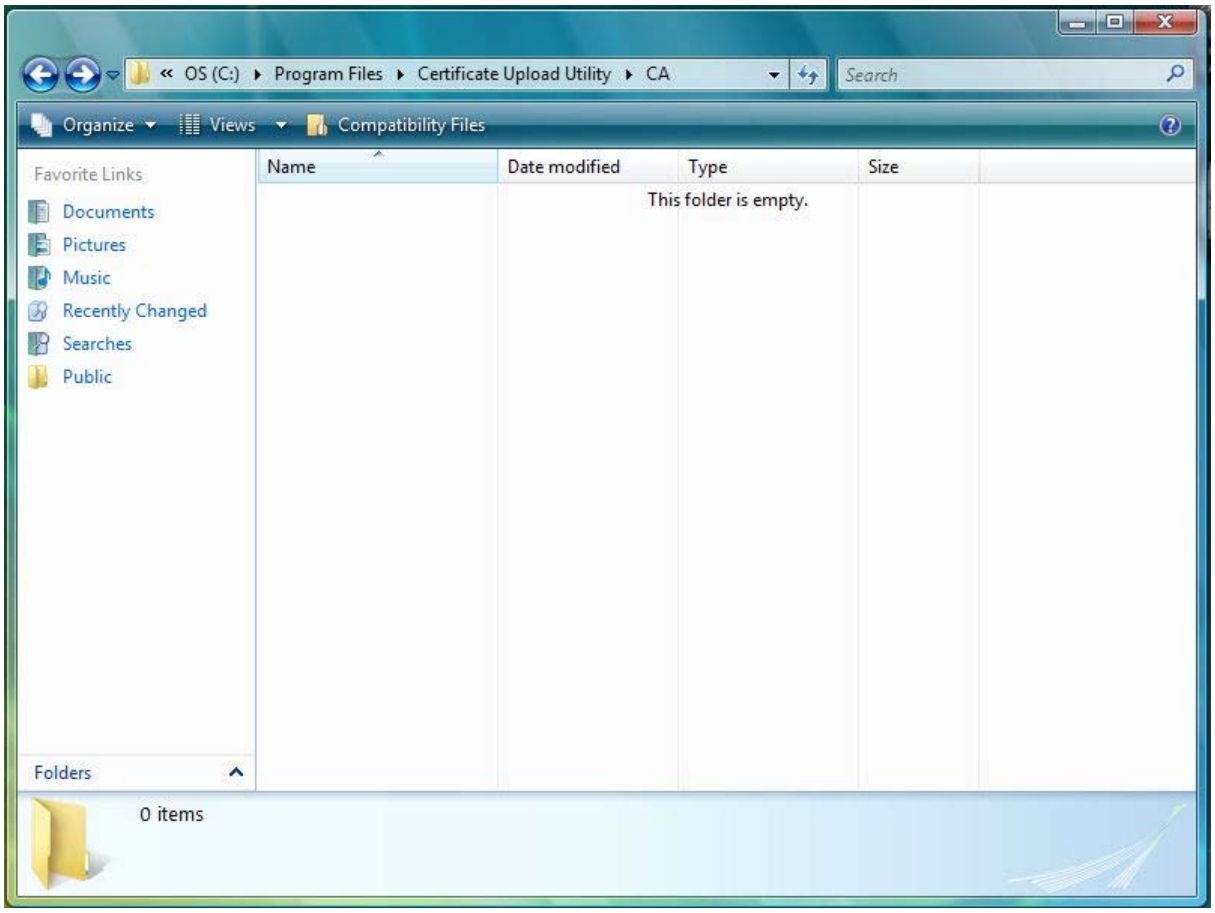
Repeat Step 4 for each iBootBar.

All PCs with the same Root Authority Certificate installed will be able to Create and upload certificates to any iBootBars, and to access all the iBootBars with certificates made from that same Root Authority Certificate, regardless of which PC created the certificate.

Appendix A

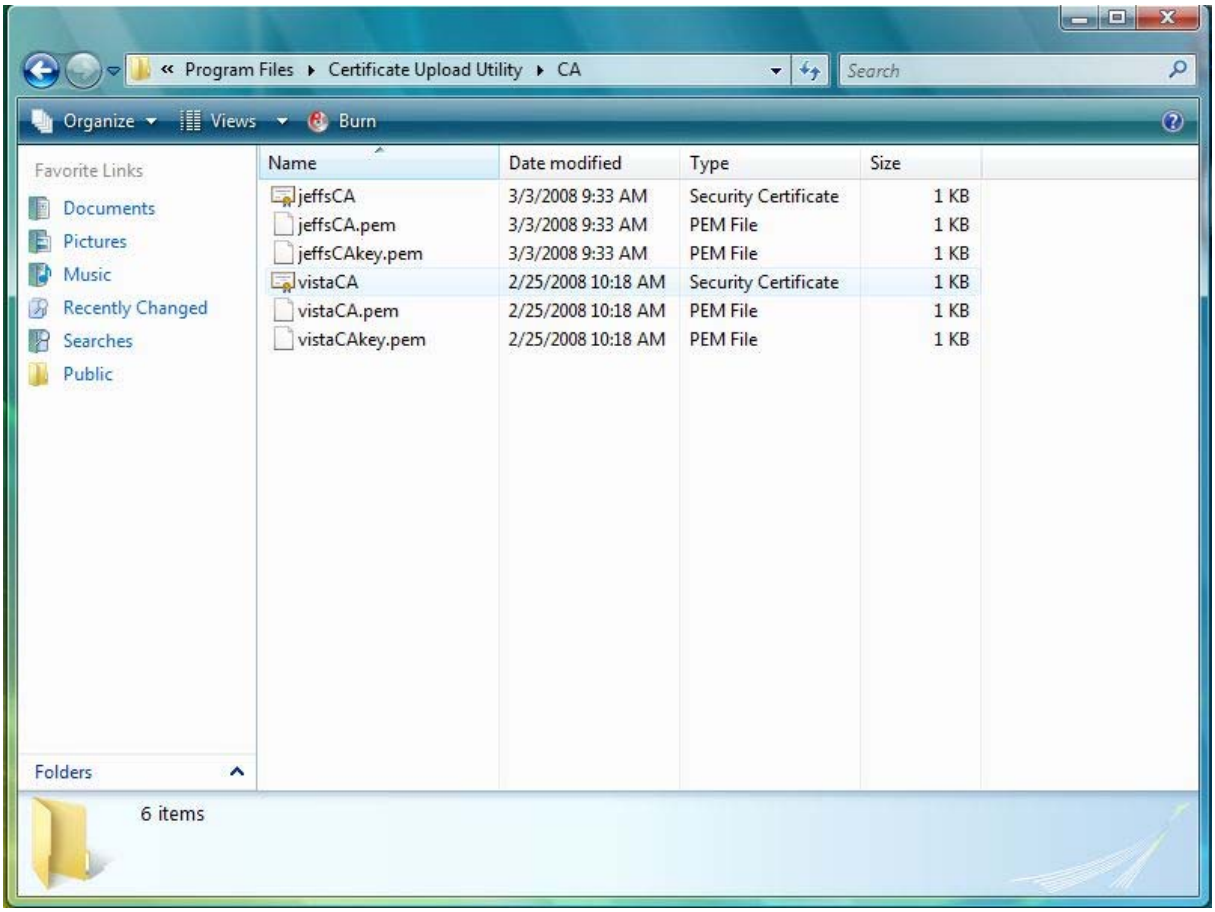
CU Vista Compatibility Files

The Windows Vista Operating system will not allow programs to write to any directory in the “Program Files” directory. It stores them in a Virtual Store location on the hard drive. This does not prevent CU from locating them when uploading the compiled certificates. It does, however, hide them from Windows Explorer as shown below:



In this picture no virtually stored files are shown. To gain access to the Certificates stored in this directory simply click on Compatibility Files. This feature is only available to the user that was logged in when the files were created.

After clicking in Compatibility Files all the files in the virtual store directory become visible and shown below:



The Security Certificate Files can now be copied to anywhere else on the computer.
The Security Certificate files are the files that can be imported into the browser.