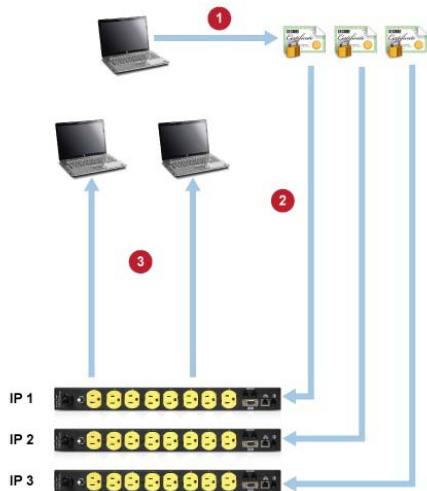


Overview

The Certificate Utility (CUU.exe) is designed to create and distribute Secure Socket Layer (SSL) certificates to iControls and the PCs that communicate with them. Although the iControl comes from the factory with a certificate installed, this certificate will generate a warning message when connecting to the iControl when using SSL. For most customers, this error message can be easily ignored and secure connection to the iControl continues. For customers with special circumstances, the CU was designed to facilitate creation and distribution of SSL Certificates tailored to a specific iControl, 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 iControl. The CU also provides the means to install the certificate on the iControl, making it easy to generate and distribute. Upon initial connection to the iControl, the user will be offered an opportunity to install the certificate from the iControl. This is done once for each browser on the PC and each iControl.



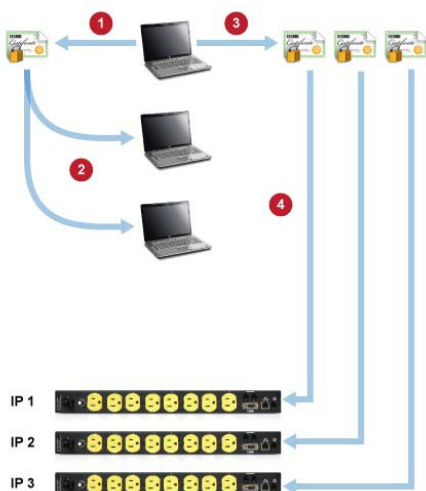
Self Sign Method

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

Step 2: Use the CU to upload the Certificates to each iControl.

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

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



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 iControls.

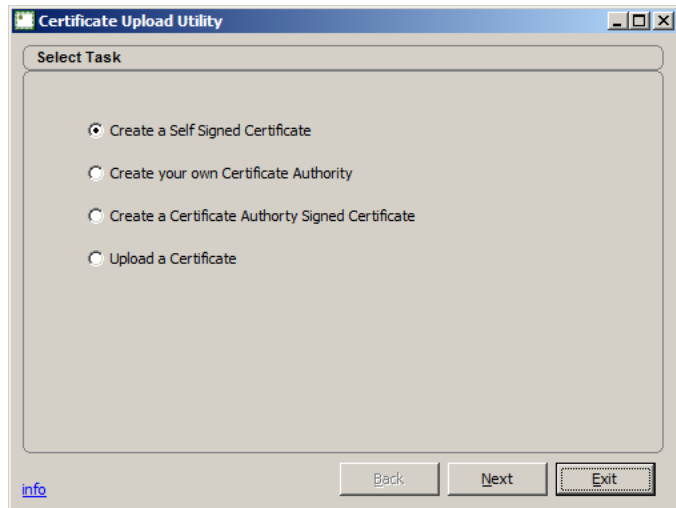
Step 3: Create certificates for each iControl using the CU. Each certificate is unique and based on the CA and the iControl's IP Address or domain name.

Step 4: Install the certificate into the iControl(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.

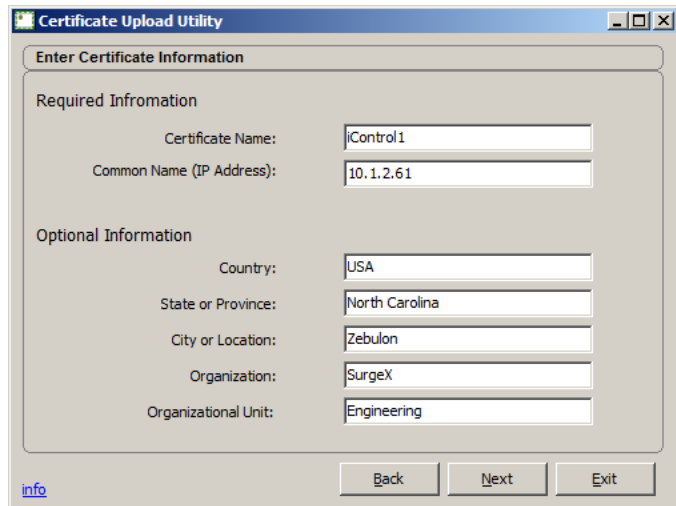


- d. Enter the Required Information about the Self Signed Certificate in the fields as shown.

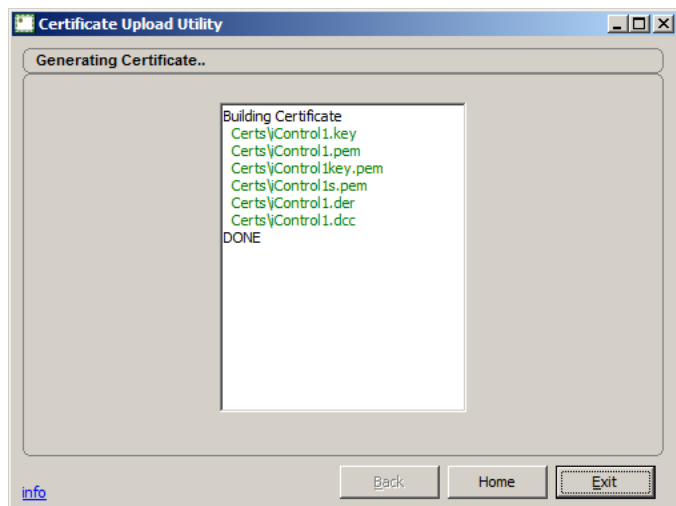
Certificate Name: This is the filename for the certificate.

Common Name: Usually the IP address of the iControl 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.

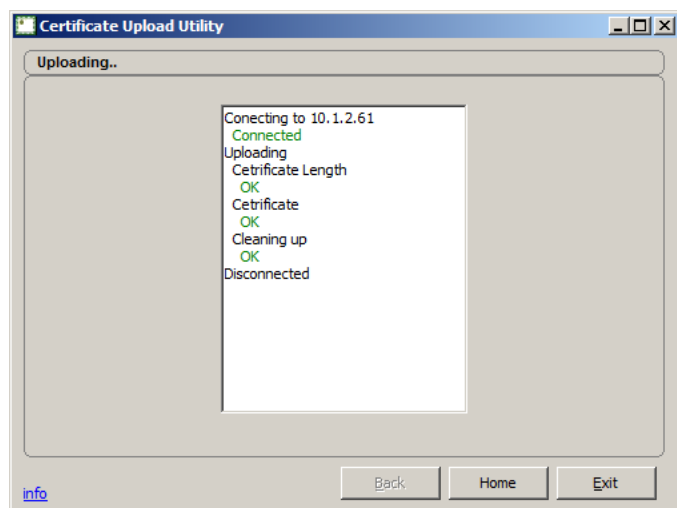
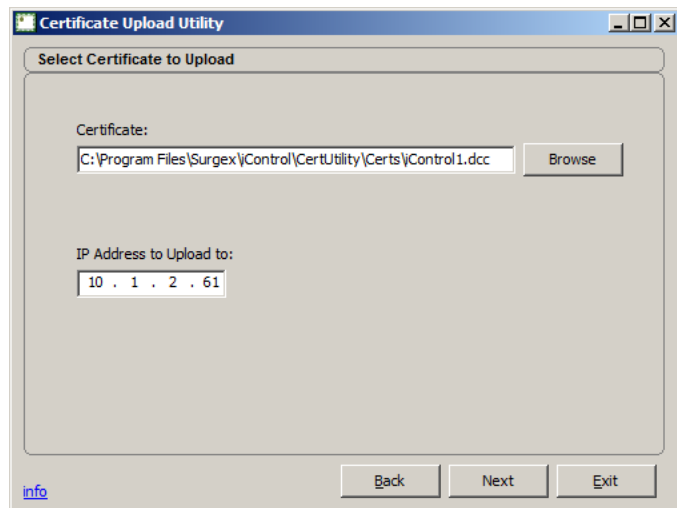
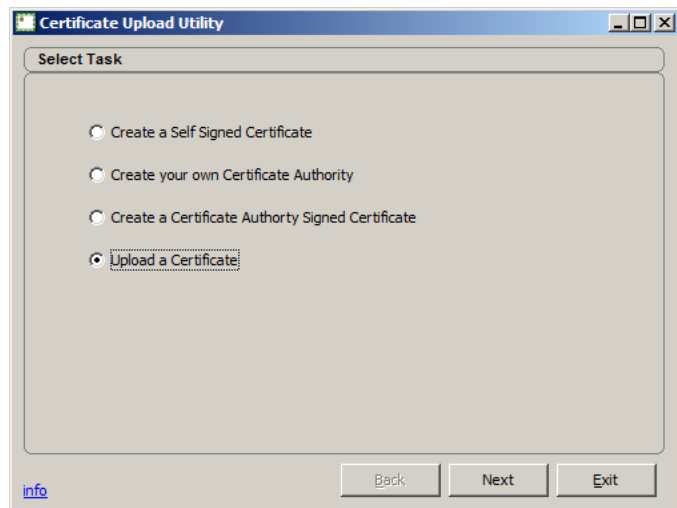


Step 2. Upload the Certificate to the iControl

- a. Open the CU.
- 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 iControl to upload the certificate to.
- f. Click on Next.

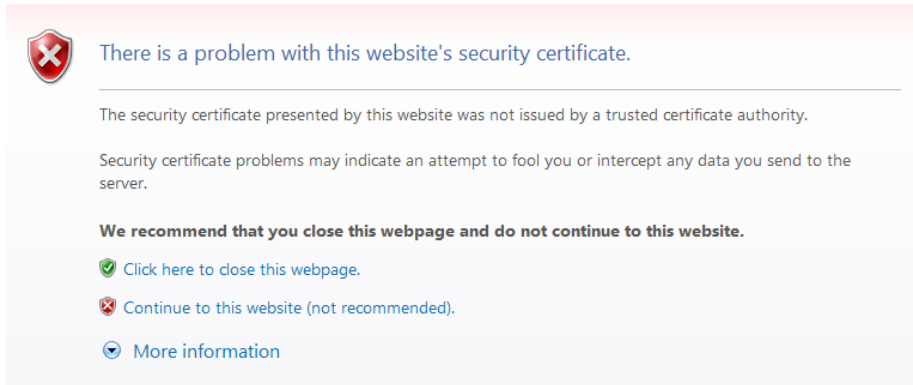
- g. The certificate upload progress is displayed. When complete, Click Home.
- h. After receiving the certificate, the iControl needs to be rebooted via the CLI (Telnet, Serial) or the front panel switch. This will not affect the status of the outlets.



Step 3. Use the Certificate in a Browser

Internet Explorer

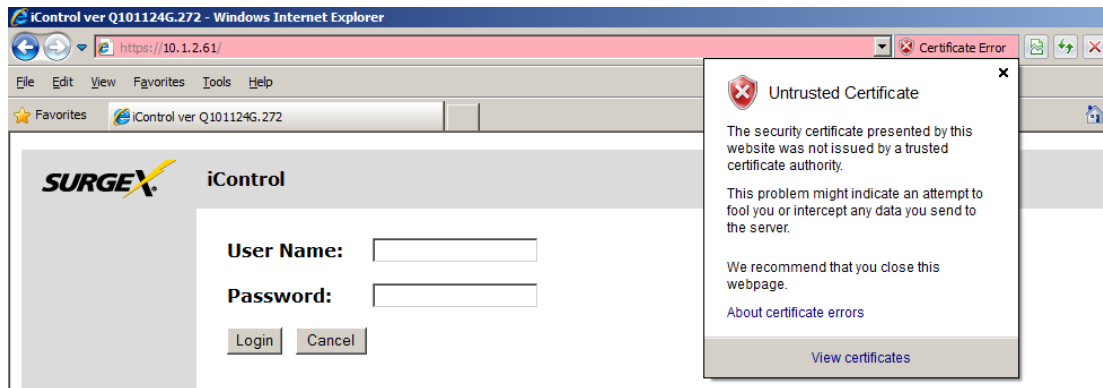
Upon connection to the iControl with the new certificate (Note: The address must now be specified as **https://ipaddress**), the following warning will be displayed:



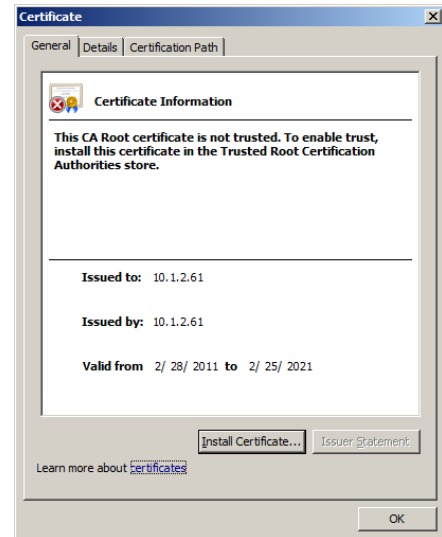
If you click “Continue to this website”: The certificate will be installed for this session only. Each time you access this iControl, the same warning will be displayed.

To permanently install this certificate:

- a. Click “Continue to this website”.
- b. Click “Certificate Error” to the right of the address bar, and click “View Certificates”.

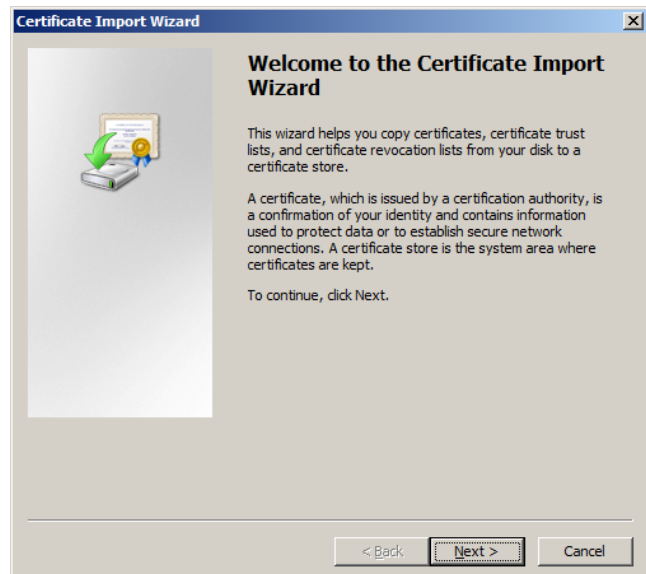


c. Click “Install Certificate”.

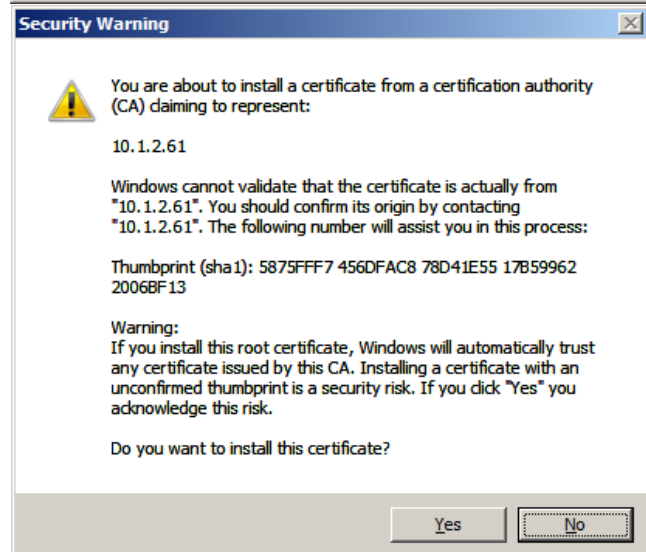


d. The import wizard will begin. Click “Next”.

e. Select “Place all certificates in the following store”, and then click “Browse”, select “Trusted Root Certification Authorities”, and click “Ok”. Click “Next”, then click “Finish”.

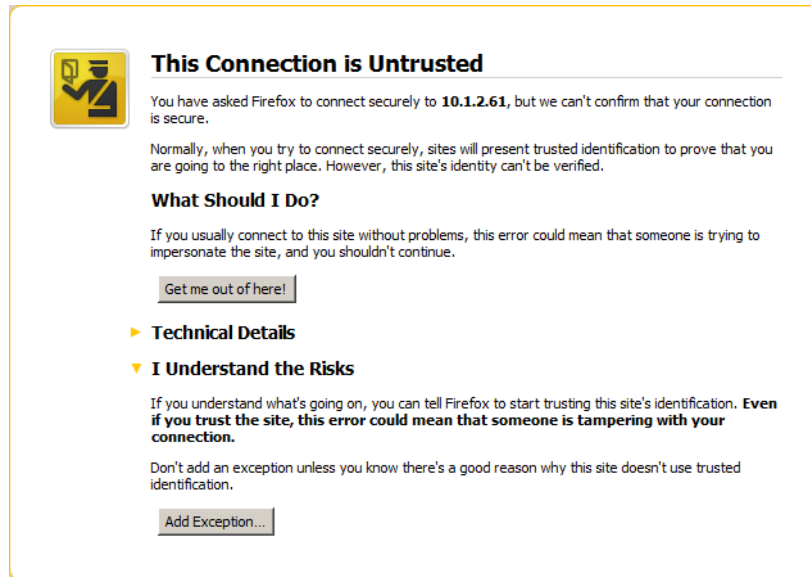


f. Review and accept the Security Warning. Click “Yes” to install the certificate permanently.



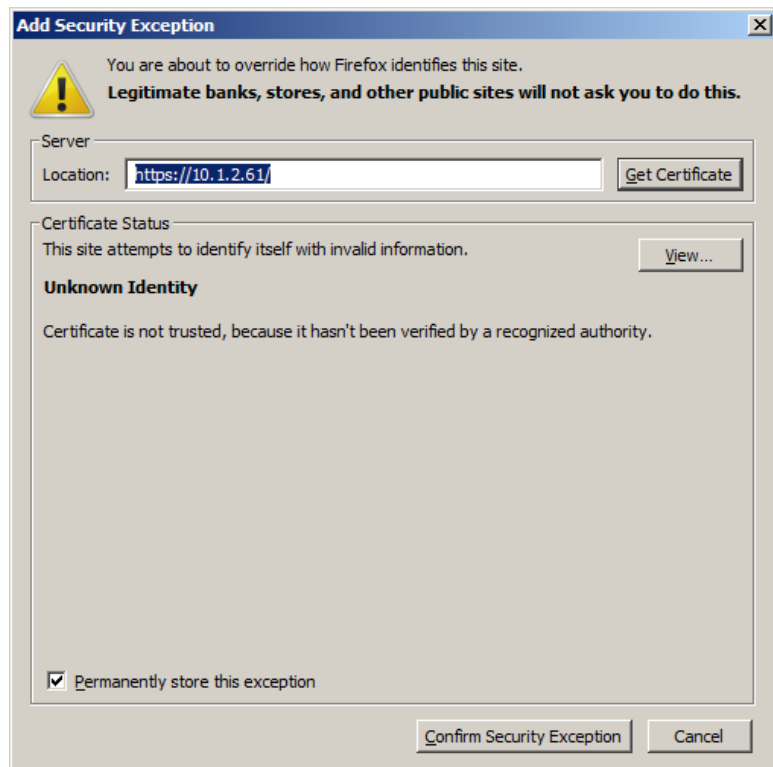
Firefox

Upon connection to the iControl with the new certificate (Note: The address must now be specified as **https://ipaddress**), the following warning will be displayed:




Click “I Understand the Risks”, and then click “Add Exception”.

On the “Add Security Exception” window that appears, click “Confirm Security Exception”. To permanently install this certificate, check the box beside “Permanently store this exception”.



Chrome

Upon connection to the iControl with the new certificate (Note: The address must now be specified as **https://ipaddress**), the following warning will be displayed:



The site's security certificate is not trusted!

You attempted to reach **10.1.2.61**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications. You should not proceed, **especially** if you have never seen this warning before for this site.

▶ [Help me understand](#)

If you click “Proceed anyway”: The certificate will be installed for this session only. Each time you access this iControl, the same warning will be displayed.

To permanently install this certificate, follow the instructions for Internet Explorer (above) to install this certificate in the Trusted Root Certification Authorities Store.

Method 2: Root Certificate Authority

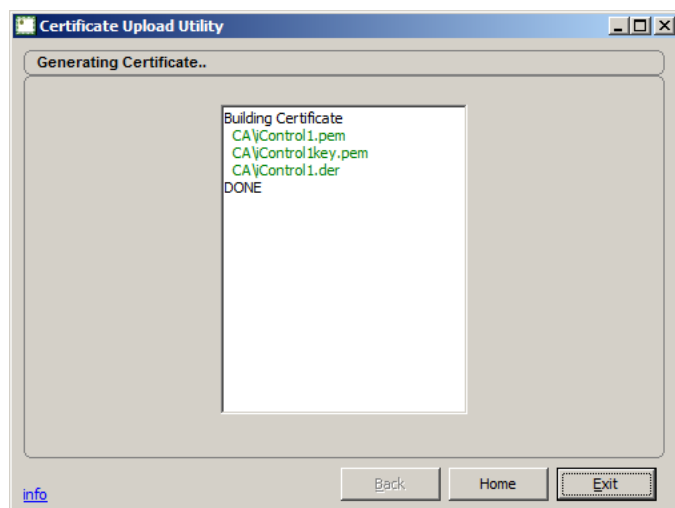
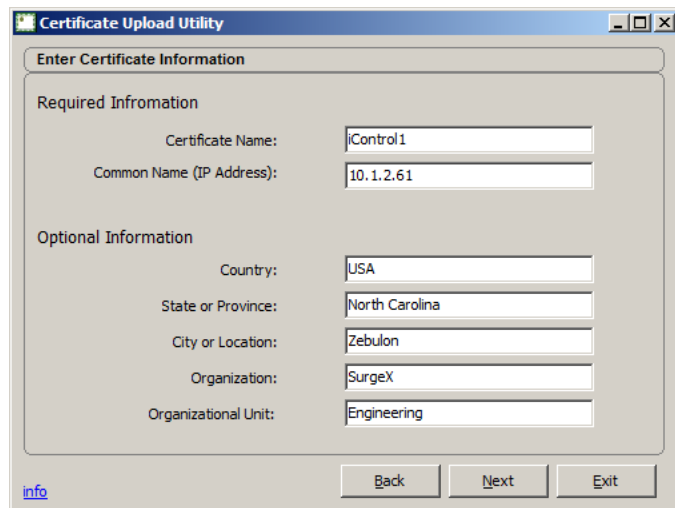
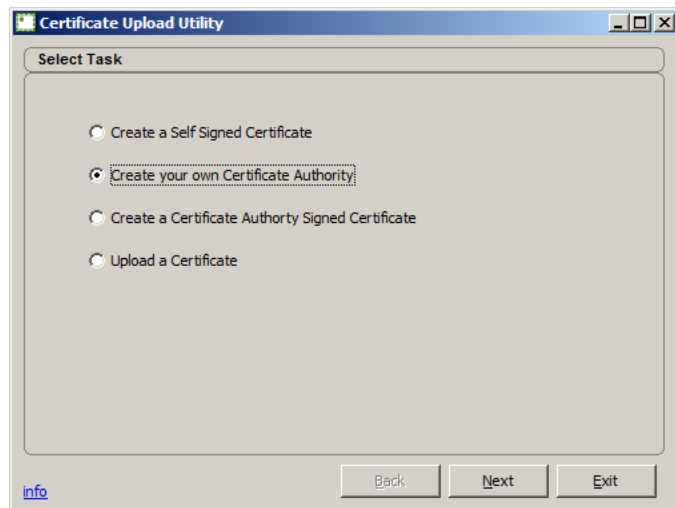
Step 1. Create a Root Certificate Authority

- 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.

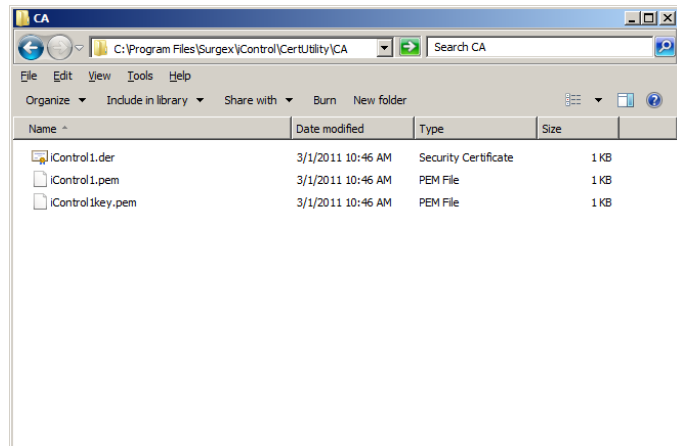
Common Name: This name identifies the Certificate to the web browser. Choose a name that will identify its source.

- 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 your browser.

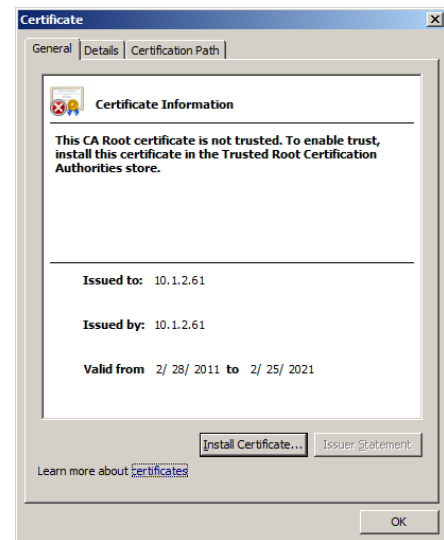


Step 2. Install the Root Authority Certificate into one or more PCs Using Internet Explorer

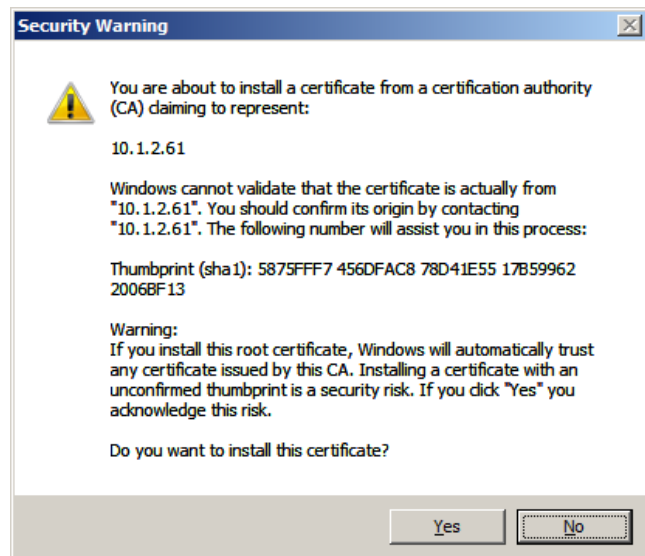
- a. Navigate to the location of the Root Certificate.
- b. Double-click on the .der file matching the filename of the certificate.



- c. Click “Install Certificate”.
- d. The import wizard will begin. Click “Next”.
- e. Select “Place all certificates in the following store”, and then click “Browse”, select “Trusted Root Certification Authorities”, and click “Ok”. Click “Next”, then click “Finish”.



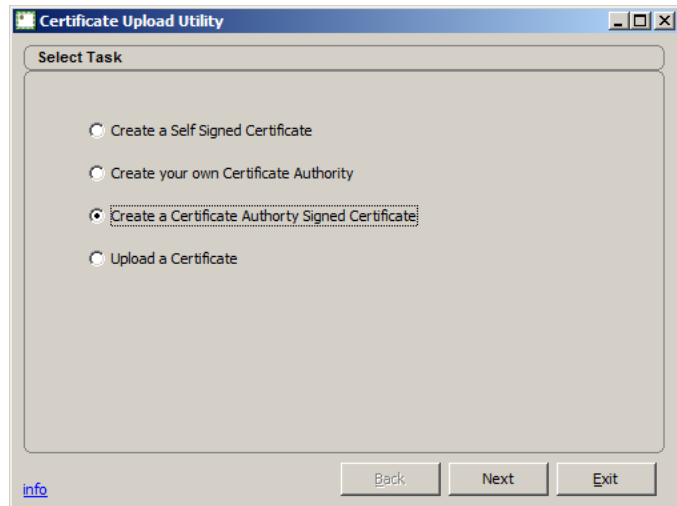
- f. Review and accept the Security Warning. Click “Yes” to install the certificate permanently.



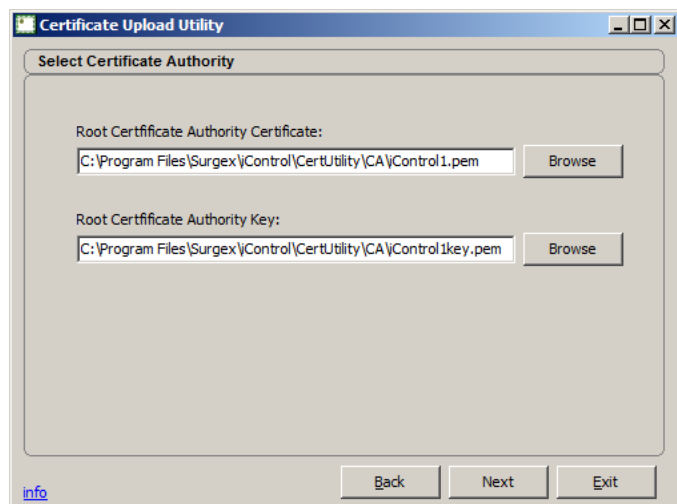
Repeat **Step 2** for all PCs that need to communicate securely with the iControls. Copy the three files created in this step to each of the PCs, and install the Root Authority Certificate in each.

Step 3. Create Certificates for each iControl 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.



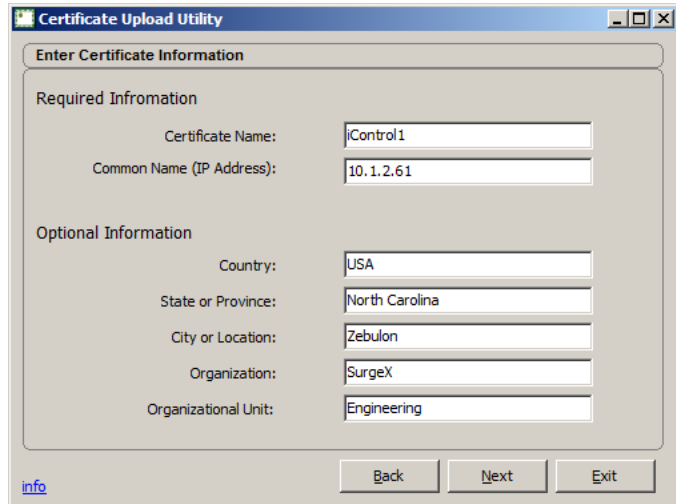
- g. Enter the Required Information about the Certificate in the fields as shown.

Certificate Name: This is the filename for the certificate.

Common Name: Usually the IP address of the iControl that will use the certificate.

- h. Enter the Optional Information if desired.

- i. Click Next when done.

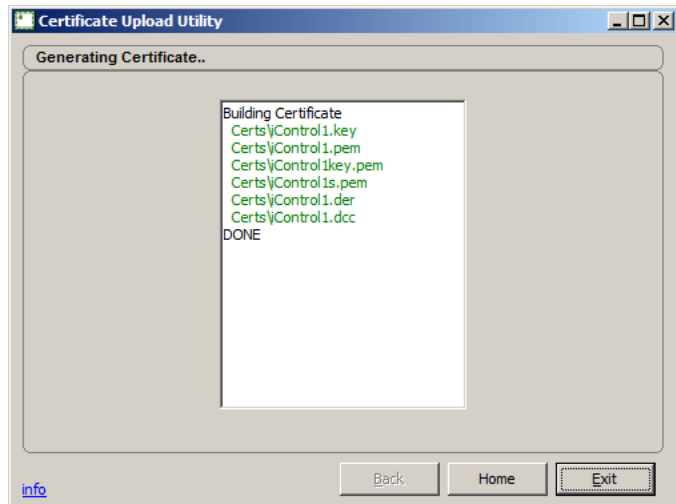


The screenshot shows the 'Certificate Upload Utility' window with the 'Enter Certificate Information' dialog box. It is divided into two sections: 'Required Information' and 'Optional Information'. The 'Required Information' section has two fields: 'Certificate Name' with the value 'iControl1' and 'Common Name (IP Address)' with the value '10.1.2.61'. The 'Optional Information' section has five fields: 'Country' with 'USA', 'State or Province' with 'North Carolina', 'City or Location' with 'Zebulon', 'Organization' with 'SurgeX', and 'Organizational Unit' with 'Engineering'. At the bottom right, there are three buttons: 'Back', 'Next', and 'Exit'. An 'info' link is visible at the bottom left.

- 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 iControl.

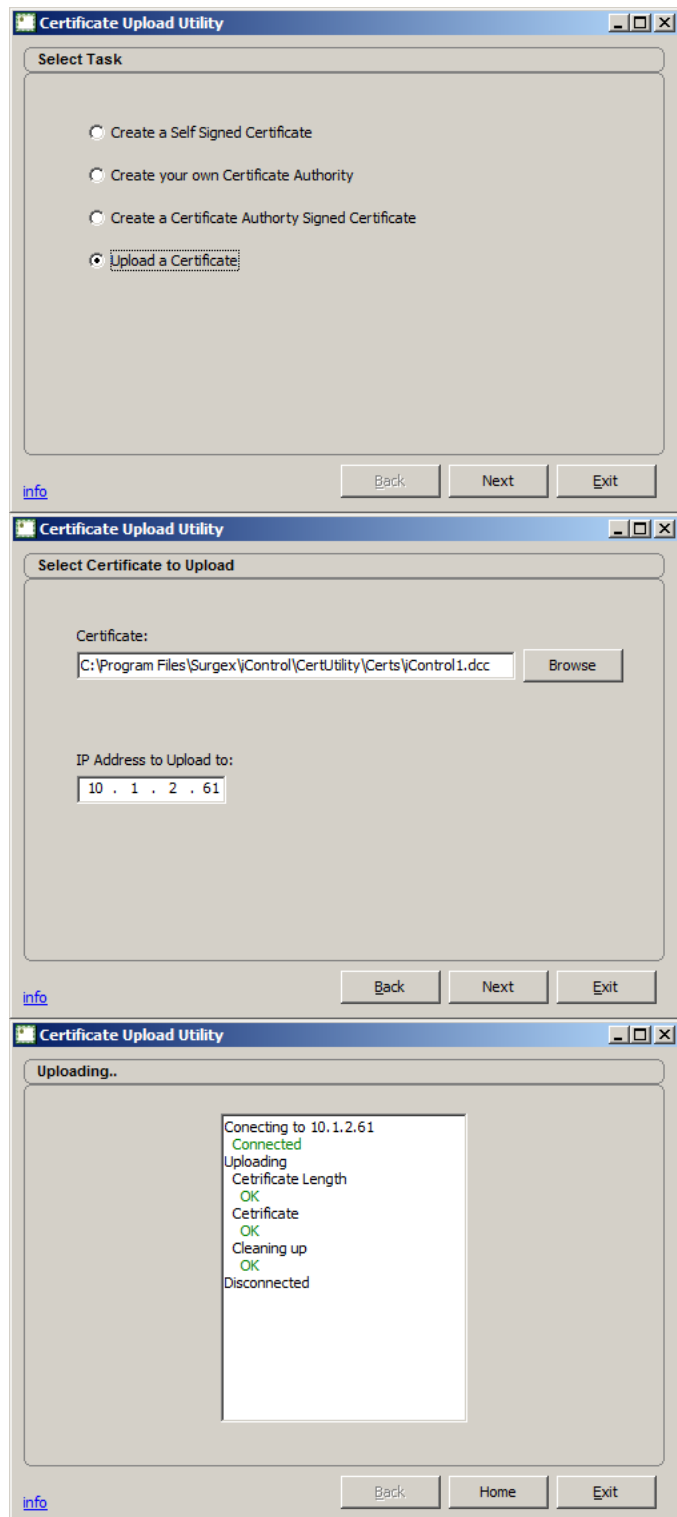


The screenshot shows the 'Certificate Upload Utility' window with the 'Generating Certificate..' dialog box. A text area displays the following output: 'Building Certificate', 'Certs\\Control1.key', 'Certs\\Control1.pem', 'Certs\\Control1key.pem', 'Certs\\Control1s.pem', 'Certs\\Control1.der', 'Certs\\Control1.dcc', and 'DONE'. At the bottom right, there are three buttons: 'Back', 'Home', and 'Exit'. An 'info' link is visible at the bottom left.

Step 4. Upload the Certificate into the iControl.

- a. Open the CU.
- b. Click 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 iControl 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 iControl needs to be rebooted via the CLI (Telnet, Serial) or the front panel switch. This will not affect the status of the outlets.

Repeat **Step 4** for each iControl.



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